



Acronis Backup & Recovery 11.5

Update 2

Benutzeranleitung

Gilt für folgende Editionen:

- ☑ Advanced Server
- ☑ Virtual Edition
- ☑ Advanced Server SBS Edition
- ☑ Advanced Workstation
- ☐ Für Microsoft Exchange Server
- ☑ Für Microsoft SQL Server (Single-Pass)
- ☑ Für Microsoft Active Directory (Single-Pass)
- ☐ Server für Windows
- ☐ Server für Linux
- ☐ Workstation

Urheberrechtserklärung

Von Acronis patentierte Technologien

Die in diesem Produkt verwendeten Technologien werden durch folgende Patente abgedeckt: U.S. Patent # 7,047,380; U.S. Patent # 7,246,211; U.S. Patent # 7,318,135; U.S. Patent # 7,366,859; U.S. Patent # 7,636,824; U.S. Patent # 7,831,789; U.S. Patent # 7,886,120; U.S. Patent # 7,934,064; U.S. Patent # 7,949,635; U.S. Patent # 7,979,690; U.S. Patent # 8,069,320; U.S. Patent # 8,073,815; U.S. Patent # 8,074,035.

Inhaltsverzeichnis

1 Einführung in Acronis Backup & Recovery 11.5

1.1 Die Neuerungen von Update 2

- Single-Pass-Backup von Microsoft Active Directory-Daten (S. 356)
    - Einen Domain-Controller zu einem beliebigen Backup-Ziel (einschließlich dem Acronis Online Backup Storage) sichern.
    - Einen kompletten Domain-Controller ohne das Risiko eines USN-Rollbacks wiederherstellen.
    - Microsoft Active Directory-Daten aus bzw. von einem Backup extrahieren und beschädigte Daten mit einigen einfachen Schritten ersetzen.
- Exchange 2013-Postfächer (und deren Inhalte) von Datenbank-Backups (als Quelle) zu .pst-Dateien (als Ziel) wiederherstellen.
- Es gibt nun für Acronis Backup & Recovery Online auch 'Abonnements für mehrere Systeme'.
- Unterstützung von WinPE 5.0.
- Unterstützung für Ubuntu 13.10.

1.2 Die Neuerungen von Update 1

Mit Build 37975 hinzugekommene Verbesserungen

- Basis-Unterstützung für Windows 8.1 und Windows Server 2012 R2.
- Installation von Acronis Backup & Recovery 11.5 im Testmodus ohne einen Lizenzschlüssel.
- Upgrade von einem Standalone-Produkt zur Advanced-Plattform, ohne dass die Software neu installiert werden muss.
- Backup und Recovery mit dem Agenten für ESX(i): VMware vSphere 5.5.
- Backup und Recovery innerhalb eines Gastsystems: Red Hat Enterprise Virtualization 3.2, Oracle VM VirtualBox 4.x.
- Unterstützung für Linux-Kernel bis Version 3.9
- Unterstützung für Ubuntu 12.10, 13.04 und Fedora 18.

Zusätzliche Unterstützung für Microsoft Exchange Server 2013 (beginnend mit Build 37687)

- Backup und Recovery von Microsoft Exchange Server 2013-Datenbanken mit dem Agenten für Exchange. Backup und Recovery von Exchange 2013-Postfächern (einschließlich Postfach-Recovery von Datenbank-Backups) werden derzeit noch nicht unterstützt, werden aber mit zukünftigen Updates hinzugefügt.
- Das Kumulative Update 1 für Microsoft Exchange Server 2013 und später wird unterstützt.

Single-Pass-Backups von Microsoft SQL Server-Daten (S. 345)

- Verwenden Sie eine einzelne Lösung und einen einzelnen Backup-Plan gleichermaßen für Desaster-Recovery wie zum Schutz von Daten.
- Sichern Sie eine Maschine per Backup und stellen Sie Laufwerke, Volumes, Dateien oder Microsoft SQL-Datenbanken wieder her.
- Stellen Sie Microsoft SQL-Datenbanken direkt zu einer laufenden SQL Server-Instanz wieder her oder extrahieren Sie die Datenbanken als Dateien in ein Dateisystem.
- Führen Sie eine SQL Server-Protokollabschneidung direkt nach einem Backup durch.

- Verwenden Sie jedes Backup-Ziel, einschließlich des Acronis Online Backup Storages.
- Microsoft SQL Server 2012 wird unterstützt, genauso wie frühere Microsoft SQL Server-Versionen.

Basis-Unterstützung für Windows 8 und Windows Server 2012 (S. 54)

- Installieren Sie den Agenten für Windows, den Agenten für SQL (Single-Pass) sowie Verwaltungskomponenten unter Windows 8 und Windows Server 2012.
- Booten Sie eine Maschine mit einem auf WinPE 4 basierenden Boot-Medium.
- Verwenden Sie ein bootfähiges Medium auf einer Maschine, auf der UEFI Secure Boot aktiviert ist.
- Führen Sie Backup- und Recovery-Aktionen (ohne Größenanpassung) mit Volumes durch, die das ReFS-Dateisystem verwenden oder beliebige Daten enthalten.
- Sichern Sie Speicherplätze (Storage Spaces) per Backup und stellen Sie diese am ursprünglichen Ort, zu anderen Speicherplätzen oder als gewöhnliche Laufwerke wieder her.
- Führen Sie Backup- und Recovery-Aktionen (auf Laufwerksebene) mit Volumes durch, auf denen die Datendeduplizierungsfunktion aktiviert ist.

Virtualisierung

Unterstützung für neue Virtualisierungsplattformen:

- Backup und Recovery mit dem Agenten für ESX(i): VMware vSphere 5.1.
- Backup und Recovery mit dem Agenten für Hyper-V: Hyper-V 3.0.

  Der Agent für Hyper-V kann nicht unter Windows 8 installiert werden, auch wenn dieses Betriebssystem die Hyper-V Funktionalität enthält.
- Backup und Recovery innerhalb eines Gastsystems: Oracle VM Server 3.0, Red Hat Enterprise Virtualization 3.1.

Linux

- Unterstützung für Oracle Linux 5.x, 6.x – Unbreakable Enterprise Kernel und Red Hat Compatible Kernel

Andere(s)

- Deaktivieren Sie die Backup-Katalogisierung (S. 114) vollständig auf einer verwalteten Maschine, einem Storage Node oder dem Management Server.
- Speichern Sie einen Desaster-Recovery-Plan (S. 123) in einem lokalen Ordner oder Netzwerkordner (zusätzlich zum Versenden per E-Mail).
- Aktivieren Sie VSS-Voll-Backups (S. 142), um die Protokolle von VSS-kompatiblen Anwendungen nach einem Laufwerk-Backup abschneiden zu können.
- Booten Sie eine UEFI-Maschine mit einem auf 64-Bit WinPE basierenden (S. 290) Boot-Medium.
- Fügen Sie die Variable **%description%** (entspricht der in den Systemeigenschaften einer Windows-Maschine angezeigten Beschreibung) dem Betreff für die E-Mail-Benachrichtigung (S. 131) hinzu.

1.3 Neuerungen in Acronis Backup & Recovery 11.5

Bei der Erweiterung der Backup- und Recovery-Fähigkeiten für physikalische, virtuelle und Cloud-Umgebungen hat Acronis nun auch die Backup- und Recovery-Möglichkeit für Microsoft Exchange-Server-Daten hinzugefügt.

Nachfolgend finden Sie eine Zusammenfassung der neuen Produktfunktionen und Verbesserungen.

Backup und Recovery von Microsoft Exchange-Server-Daten

Schlüsselfunktionen

- **Unterstützung von Microsoft Exchange Server 2010**

  Acronis Backup & Recovery 11.5 unterstützt den Microsoft Exchange Server 2010 sowie den Microsoft Exchange Server 2003/2007.

- **Express-Voll-Backup-Methode**

  Diese Methode basiert auf der Überwachung von Änderungen an den Exchange-Datenbankdateien. Sobald das anfängliche Voll-Backup erfasst wurde, sichern alle nachfolgenden Backups nur noch Änderungen an dieser Datenbank, ohne dass dabei die komplette Datenbankdatei gelesen werden muss. Durch Kombination dieser Methode mit der Datendeduplizierungsfunktionalität können Backups von großen Datenbanken mit 1 TB und mehr während der Geschäftszeiten und sogar über WANs erstellt werden.

- **Unterstützung für Exchange-Clustering**

  Acronis Backup & Recovery 11.5 unterstützt SCC-, CCR- und DAG-Cluster-Konfigurationen. Sie können wählen, ob für eine minimale Produktionsbeeinflussung Datenbankreplikate statt der aktiven Datenbank gesichert werden sollen. Wird die Postfachrolle aufgrund von Wechsel oder Ausfallssicherung (Switchover oder Failover) zu einem anderen Server verschoben, dann verfolgt die Software alle Standortverlagerungen der Daten und schützt diese sicher per Backup.

- **Kontinuierliche Datensicherung (CDP)**

  Durch die Verwendung der kontinuierlichen Datensicherung (CDP, Continuous Data Protection) können Sie Exchange-Daten zu fast jedem Zeitpunkt hin zurückversetzen. Falls die aktuellste Transaktionsprotokolldatei überlebt hat, können Sie die Exchange-Daten zum Zeitpunkt der Fehlfunktion hin zurückversetzen.

- **Backup-Ziele**

  Backups können zu jedem von Acronis Backup & Recovery 11.5 unterstützten Storage-Typ gesichert werden, mit Ausnahme des Acronis Online Backup Storages, der Acronis Secure Zone und von Wechselmedien.

- **Erweitertes granuläres Recovery**

  Durchsuchen Sie Exchange-Server-Datenbanken oder Postfach-Backups und stellen Sie einzelne bzw. mehrere Postfächer oder bestimmte E-Mails wieder her. Sie können außerdem Kalenderelemente, Notizen, Aufgaben und Journaleinträge wiederherstellen.

- **Neue Recovery-Ziele**

  Neben der Möglichkeit, Daten auch zu einem aktiven Exchange-Server wiederherzustellen, sind außerdem folgende Wiederherstellungen möglich:

  - Exchange-Datenbanken zu normalen Laufwerksordnern.
  - E-Mails und Postfächer zu .pst-Dateien.

Virtualisierung

- **Unterstützung für UEFI-basierte virtuelle Maschinen (S. 53)** (gilt nur für VMware ESXi 5)

  Backup und Recovery von virtuellen Maschinen, die UEFI (Unified Extensible Firmware Interface) verwenden. Konvertierung einer UEFI-basierten physikalischen Maschine (S. 190) zu einer virtuellen Maschine, welche die gleiche Boot-Firmware verwendet.

- **Recovery auf Dateiebene**

  Recovery einzelner Dateien und Ordner in das lokale Dateisystem des Agenten (nur unter Windows), zu einer Netzwerkfreigabe oder zu einem FTP- bzw. SFTP-Server.

- Unterstützung für **Changed Block Tracking (CBT)** (gilt nur für VMware ESX(i) 4.0 und höher)

Durchführung schnellerer inkrementeller und differentieller Backups von virtuellen ESX(i)-Maschinen durch die Verwendung der CBT-Funktion (Changed Block Tracking) von ESX(i).

- **Unterstützung für VM-Templates**

  Backup und Recovery von virtuellen Maschinen-Templates auf gleiche Weise wie von normalen virtuellen ESX(i)-Maschinen.

- **'Bare Metal Recovery' von Microsoft Hyper-V-Hosts**

  Backups eines kompletten Hyper-V-Hosts zusammen mit seinen virtuellen Maschinen, ohne dass seine normale Aktivität dabei unterbrochen wird. Sie können als Ziel für die Wiederherstellung des Hosts dann dieselbe oder auch abweichende Hardware verwenden.

- **Erweiterte Unterstützung für Red Hat Enterprise Virtualization-Umgebungen**

  Backup und Recovery von virtuellen Maschinen, die in einer RHEV-Umgebung laufen. Migration von physikalischen Maschinen zu einer RHEV-Umgebung (P2V); und Migration einer virtuellen Maschine von einer anderen Virtualisierungsplattform zur RHEV-Plattform (V2V).

Installation

- Remote-Installation des Acronis Backup & Recovery 11.5 Agenten für Linux.

Unterstützung für zahlreiche Storage-Typen

Acronis Online Backup Storage (nur für unter Windows laufende Maschinen und virtuelle Maschinen)

- Backups zum Acronis Online Backup Storage replizieren oder verschieben (S. 111).
- Die Backup-Schema 'Großvater-Vater-Sohn' und 'Türme von Hanoi' stehen jetzt auch bei Backups zum Acronis Online Backup Storage zur Verfügung.

Bänder (nur Advanced-Editionen)

- Für auf Bändern gespeicherte Laufwerk-Backups ist eine Wiederherstellung auf Dateiebene möglich.

  Diese Funktion kann durch Konfiguration der entsprechenden Bandverwaltungsoption (S. 138) (de)aktiviert werden.

Zentrale Verwaltung

- Depot-Auswahl im Datenkatalog (S. 150)

  Sie können das Depot, von dem aus die Daten wiederhergestellt werden sollen, auswählen, falls die Backup-Daten mehrere Replikate haben, die in mehr als einem verwalteten Depot gespeichert sind.

Linux

- **Unterstützung für Linux-Kernel bis 3.6**
- **Unterstützung für folgende Linux-Distributionen:**
  - Ubuntu 11.04, 11.10, 12.04
  - Fedora 15, 16, 17
  - Debian 6
  - CentOS 6.x
- **Unterstützung für UEFI (Unified Extensible Firmware Interface)** (S. 53)

  Erstellen Sie ein Backup von einer UEFI-basierten, unter Linux laufenden Maschine und stellen Sie dieses auf derselben oder einer anderen UEFI-basierten Maschine wieder her.

Bootfähiges Medium

- Neue Linux-Kernel-Version (3.4.5) bei Linux-basierten bootfähigen Medien. Der neue Kernel bringt eine bessere Hardware-Unterstützung mit sich.

Benutzeroberfläche

- Unterstützung für eine Bildschirmauflösung von 800x600

1.4 Acronis Backup & Recovery 11.5-Komponenten

Dieser Abschnitt enthält eine vollständige Liste der Acronis Backup & Recovery 11.5-Komponenten mit einer kurzen Beschreibung ihrer Funktion.

Acronis Backup & Recovery 11.5 enthält die drei folgenden Haupttypen von Komponenten.

Komponenten für eine verwaltete Maschine (Agenten)

Dies sind Anwendungen zur Durchführung von Backups, Wiederherstellungen und anderen Aktionen auf Maschinen, die mit Acronis Backup & Recovery 11.5 verwaltet werden. Die Agenten benötigen je eine Lizenz zur Durchführung von Aktionen mit einer verwalteten Maschine. Agenten haben mehrere Features (Add-ons), die zusätzliche Funktionen ermöglichen und daher möglicherweise weitere Lizenzen erfordern.

Komponenten zur zentralen Verwaltung

Diese mit den Advanced-Editionen ausgelieferten Komponenten bieten die Fähigkeit zur zentralen Verwaltung. Zur Verwendung dieser Komponenten wird keine Lizenz benötigt.

Konsole

Die Konsole bietet eine grafische Benutzeroberfläche sowie eine Remote-Verbindung mit den Agenten und anderen Acronis Backup & Recovery 11.5-Komponenten. Zur Verwendung der Konsole wird keine Lizenz benötigt.

Bootable Media Builder

Mit dem 'Bootable Media Builder' können Sie bootfähige Medien erstellen, damit Sie die Agenten und andere Notfallwerkzeuge in einer autonomen Notfallversion verwenden können.

Der Bootable Media Builder erfordert keine Lizenz, wenn er zusammen mit einem Agenten installiert wird. Alle Add-ons für den Agenten stehen, sofern installiert, auch in der Notfallumgebung zur Verfügung. Um einen Media Builder auf einer Maschine ohne Agenten nutzen zu können, müssen Sie einen Lizenzschlüssel eingeben oder wenigstens eine Lizenz auf dem License Server verfügbar haben. Die Lizenz kann entweder verfügbar oder zugewiesen sein.

1.4.1 Agent für Windows

Dieser Agent ermöglicht unter Windows, Ihre Daten auf Laufwerk- und Datei-Ebene zu schützen.

Laufwerk-Backup

Der Schutz auf Laufwerksebene basiert auf Sicherung des gesamten Dateisystems eines Laufwerks bzw. Volumes, einschließlich aller zum Booten des Betriebssystems notwendigen Informationen; oder – beim Sektor-für-Sektor-Ansatz – auf Sicherung aller Laufwerkssektoren (raw-Modus). Ein Backup, welches die Kopie eines Laufwerks oder Volumes in gepackter Form enthält, wird auch Laufwerk-Backup (Disk-Backup, Partition-Backup, Volume-Backup) oder Laufwerk-Image

(Partition-Image, Volume-Image) genannt. Aus solchen Backups können Laufwerke oder Volumes komplett wiederhergestellt werden – aber auch einzelne Dateien oder Ordner.

Datei-Backup

Der Schutz der Daten auf Datei-Ebene basiert auf der Sicherung von Dateien und Ordnern, die sich auf der Maschine, auf der der Agent installiert ist oder auf einem freigegebenen Netzlaufwerk befinden. Dateien können an ihren ursprünglichen oder einen anderen Speicherort wiederhergestellt werden. Es ist möglich, alle gesicherten Dateien und Verzeichnisse wiederherzustellen. Sie können aber auch auswählen, welche Dateien und Verzeichnisse wiederhergestellt werden sollen.

Andere Aktionen

Konvertierung zu einer virtuellen Maschine

Der Agent für Windows führt die Konvertierung durch, indem er ein Laufwerk-Backup zu einer neuen virtuellen Maschine folgenden Typs wiederherstellt (wahlweise): VMware Workstation, Microsoft Virtual PC, Citrix XenServer Open Virtual Appliance (OVA) oder Red Hat KVM (Kernel-based Virtual Machine). Die Dateien der vollständig konfigurierten und einsatzbereiten Maschine werden in dem von Ihnen ausgewählten Ordner abgelegt. Sie können die Maschine unter Verwendung der entsprechenden Virtualisierungssoftware starten oder die Dateien der Maschine für eine zukünftige Verwendung vorbereiten.

Laufwerksverwaltung

Agent für Windows enthält Acronis Disk Director Lite - ein nützliches Werkzeug zur Laufwerksverwaltung. Aktionen zur Laufwerksverwaltung, wie das Klonen und Konvertieren von Laufwerken, das Erstellen, Formatieren und Löschen von Volumes; das Ändern des Partitionierungsschemas eines Laufwerks zwischen MBR und GPT oder das Ändern einer Laufwerksbezeichnung können sowohl im Betriebssystem als auch durch Nutzung eines bootfähigen Mediums durchgeführt werden.

1.4.1.1 Universal Restore

Das Add-on für Universal Restore bietet Ihnen die Möglichkeit, auf der Maschine, auf der der Agent installiert ist, die Funktion zur Wiederherstellung auf abweichender Hardware zu verwenden – und bootfähige Medien mit dieser Funktion zu erstellen. Universal Restore handhabt Abweichungen bei Geräten, die kritisch für den Betriebssystemstart sind, wie beispielsweise Speicher-Controller, Hauptplatine oder Chipsatz.

1.4.1.2 Deduplizierung

Dank dieses Add-ons kann der Agent Daten in einem deduplizierenden Depot sichern, das vom Acronis Backup & Recovery 11.5 Storage Node verwaltet wird.

1.4.2 Agent für Microsoft SQL Server (Single-Pass)

Der Acronis Backup & Recovery 11.5 Agent für Microsoft SQL Server (Single-Pass) ermöglicht Ihnen, Single-Pass-Laufwerk- und Anwendungs-Backups zu erstellen und Microsoft SQL-Datenbanken von diesen wiederherzustellen. Die Datenbanken können direkt zu einer laufenden SQL Server-Instanz wiederhergestellt oder einem Ordner im Dateisystem extrahiert werden.

Der Agent verwendet Microsoft VSS, um die Konsistenz der gesicherten Datenbanken zu gewährleisten. Der Agent kann nach einem erfolgreichen Backup das SQL Server-Transaktionsprotokoll abschneiden.

Der Agent wird als Add-on für den Agenten für Windows (S. 14) installiert.

Der Acronis Backup & Recovery 11.5 Agent für Microsoft SQL Server (Single-Pass) wird in diesem Dokument auch einfach nur als Agent für SQL (Single-Pass) bezeichnet.

1.4.3 Agent für Microsoft Active Directory (Single-Pass)

Der Acronis Backup & Recovery 11.5 Agent für Microsoft Active Directory (Single-Pass) ermöglicht Ihnen, Single-Pass-Laufwerk-Backups und applikationskonforme Backups zu erstellen – und aus diesen dann Microsoft Active Directory-Daten in bzw. zu einem Ordner in einem Dateisystem zu extrahieren.

Der Agent verwendet Microsoft VSS, um die Konsistenz der gesicherten Daten zu gewährleisten.

Der Agent wird als Add-on für den Agenten für Windows (S. 14) installiert.

Der Acronis Backup & Recovery 11.5 Agent für Microsoft Active Directory (Single-Pass) wird in diesem Dokument auch einfach nur als Agent für Active Directory (Single-Pass) bezeichnet.

1.4.4 Agent für Linux

Dieser Agent ermöglicht unter Linux, Ihre Daten auf Laufwerk- und Dateiebene zu schützen.

Laufwerk-Backup

Dabei basiert die Datensicherung auf Laufwerkebene auf der Sicherung des gesamten Dateisystems auf einem Laufwerk bzw. einem Volume, einschließlich aller zum Booten des Betriebssystems notwendigen Informationen; oder – bei einem Sektor-für-Sektor-Ansatz – auf der Sicherung der einzelnen Sektoren (raw-Modus). Ein Backup, welches die Kopie eines Laufwerks oder Volumes in gepackter Form enthält, wird auch Laufwerk-Backup (Disk-Backup, Partition-Backup, Volume-Backup) oder Laufwerk-Image (Partition-Image, Volume-Image) genannt. Aus solchen Backups können Laufwerke oder Volumes komplett wiederhergestellt werden – aber auch einzelne Dateien oder Ordner.

Datei-Backup

Die Datensicherung auf Datei-Ebene basiert auf der Sicherung von Dateien und Verzeichnissen, die sich auf der Maschine, auf der der Agent installiert ist oder auf einem freigegebenen Netzlaufwerk befinden, auf das über das SMB- oder das NFS-Protokoll zugegriffen wird. Dateien können an ihren ursprünglichen oder einen anderen Speicherort wiederhergestellt werden. Es ist möglich, alle gesicherten Dateien und Verzeichnisse wiederherzustellen. Sie können aber auch auswählen, welche Dateien und Verzeichnisse wiederhergestellt werden sollen.

Konvertierung zu einer virtuellen Maschine

Der Agent für Linux führt die Konvertierung durch, indem er ein Laufwerk-Backup zu einer neuen virtuellen Maschine folgenden Typs wiederherstellt (wahlweise): VMware Workstation, Microsoft Virtual PC, Citrix XenServer Open Virtual Appliance (OVA) oder Red Hat KVM (Kernel-based Virtual Machine). Die Dateien der vollständig konfigurierten und einsatzbereiten Maschine werden in dem von Ihnen ausgewählten Ordner abgelegt. Sie können die Maschine unter Verwendung der

entsprechenden Virtualisierungssoftware starten oder die Dateien der Maschine für eine zukünftige Verwendung vorbereiten.

1.4.4.1 Universal Restore

Das Add-on für Universal Restore bietet Ihnen die Möglichkeit, auf der Maschine, auf der der Agent installiert ist, die Funktion zur Wiederherstellung auf abweichender Hardware zu verwenden – und bootfähige Medien mit dieser Funktion zu erstellen. Universal Restore handhabt Abweichungen bei Geräten, die kritisch für den Betriebssystemstart sind, wie beispielsweise Speicher-Controller, Hauptplatine oder Chipsatz.

1.4.4.2 Deduplizierung

Dank dieses Add-ons kann der Agent Daten in einem deduplizierenden Depot sichern, das vom Acronis Backup & Recovery 11.5 Storage Node verwaltet wird.

1.4.5 Agent für VMware vSphere ESX(i)

Der Acronis Backup & Recovery 11.5 Agent für VMware vSphere ESX(i) ermöglicht Backup und Recovery von virtuellen ESX(i)-Maschinen, ohne Agenten in den Gastsystemen installieren zu müssen. Diese Backup-Methode ist auch unter der Bezeichnung 'agentenloses Backup' oder 'Backup auf Hypervisor-Ebene' bekannt.

Der Agent wird in zwei Versionen ausgeliefert:

- Der Agent für VMware vSphere ESX(i) (Virtuelle Appliance) kann in bzw. auf einen VMware ESX(i)-Host importiert bzw. bereitgestellt werden.
- Für 'off-loaded' (Serverlast-reduzierende) Backups kann der Agent für VMware vSphere ESX(i) (Windows) auf einer unter Windows laufenden Maschine installiert werden.

Der Acronis Backup & Recovery 11.5 Agent für VMware vSphere ESX(i) wird im Verlauf dieses Dokuments auch vereinfacht als Agent für ESX(i) bezeichnet.

1.4.6 Agent für Hyper-V

Der Acronis Backup & Recovery 11.5-Agent für Hyper-V schützt virtuelle Maschinen, die sich auf einem Hyper-V-Virtualisierungsserver befinden. Der Agent ermöglicht die Sicherung virtueller Maschinen vom Host aus, ohne dass dazu Agenten auf den einzelnen virtuellen Maschinen installiert werden müssen.

Der Agent für Hyper-V kann unter folgenden Betriebssystemen installiert werden:

Windows Server 2008 (x64) mit Hyper-V

Windows Server 2008 R2 mit Hyper-V

Microsoft Hyper-V Server 2008/2008 R2

Windows Server 2012/2012 R2 mit Hyper-V

Microsoft Hyper-V Server 2012/2012 R2

Der Agent für Hyper-V kann nicht unter Windows 8/8.1 installiert werden, auch wenn dieses Betriebssystem die Hyper-V Funktionalität enthält.

1.4.7 Komponenten für zentrale Verwaltung

In diesem Abschnitt werden die Komponenten aufgeführt, die in den Acronis Backup & Recovery 11.5-Editionen enthalten sind und die Fähigkeit zur zentralen Verwaltung bieten. Zusätzlich zu diesen Komponenten müssen die Acronis Backup & Recovery 11.5-Agenten auf allen Maschinen installiert werden, auf denen Daten geschützt werden müssen.

1.4.7.1 Management Server

Acronis Backup & Recovery 11.5 Management Server ist der zentrale Server, der für die Datensicherung im Unternehmensnetzwerk sorgt. Der Management Server bietet dem Administrator:

- einen zentralen Zugriffspunkt auf die Acronis Backup & Recovery 11.5-Infrastruktur
- einen einfachen Weg zur Sicherung von Daten auf zahlreichen Maschinen (S. 493) – durch Verwendung von zentralen Backup-Plänen und Gruppierung
- Integration mit dem VMware vCenter, um virtuelle Maschinen zur Datensicherung zu ermitteln
- unternehmensweitem Monitoring und Berichtsfunktionalität
- integrierte Lizenzverwaltung
- der Fähigkeit, zentrale Depots (S. 498) zur Speicherung der Backup-Archive (S. 486) des Unternehmens zu erstellen
- der Fähigkeit, Storage Nodes (S. 495) zu verwalten
- einen zentralen Katalog (S. 488) aller Daten, die auf Storages Nodes gespeichert sind.

Gibt es mehrere Management Server im Netzwerk, dann arbeiten diese unabhängig voneinander, verwalten verschiedene Maschinen und verwenden verschiedene zentrale Depots zur Speicherung von Archiven.

1.4.7.2 Storage Node

Der Acronis Backup & Recovery 11.5 Storage Node ist ein Server, der zur optimalen Nutzung verschiedener Ressourcen entwickelt wurde (z.B. unternehmensweite Speicherkapazität, Netzwerkbandbreite oder der CPU-Last verwalteter Maschinen), welche zum Schutz bzw. zur Sicherung der Unternehmensdaten erforderlich sind. Dieses Ziel wird durch Organisation und Verwaltung der Speicherorte erreicht, die als dedizierte Speicher für die Backup-Archive des Unternehmens (verwaltete Depots) dienen.

Die wichtigste Funktion eines Storage Nodes ist die Deduplizierung (S. 259) von Backups, die in seinen Depots gespeichert sind. Was bedeutet, dass identische Daten zu einem solchen Depot nur je einmal gesichert werden. Das reduziert die Netzwerkauslastung während der Backup-Erstellung sowie den durch die Archive belegten Speicherplatz.

Die Storage Nodes ermöglichen die Schaffung einer hochgradig skalierbaren und – im Hinblick auf die unterstützte Hardware – flexiblen Speicherinfrastruktur. Es können bis zu 50 Storage Nodes eingerichtet werden, von denen jeder in der Lage ist, bis zu 20 Depots zu verwalten.

Der Administrator steuert die Storage Nodes zentral vom Acronis Backup & Recovery 11.5 Management Server (S. 18) aus. Die direkte Verbindung einer Konsole mit einem Storage Node ist nicht möglich.

1.4.7.3 Komponenten zur Remote-Installation

Es handelt sich um Installationspakete von Acronis-Komponenten, die von der Management Konsole (S. 19) zur Installation auf Remote-Maschinen verwendet werden.

Komponenten zur Remote-Installation müssen auf der Maschine mit der Konsole oder mit dem Management Server (S. 18) installiert werden. Während der Installation speichert das Setup-Programm die Komponenten an einem Standardspeicherort und speichert den Pfad zu diesem Speicherort in der Registry. Als Folge stehen die Komponenten direkt im Remote-Installationsassistenten als 'Registrierte Komponenten' zur Verfügung.

1.4.7.4 PXE Server

Der Acronis PXE Server ermöglicht es, Maschinen mit bootfähigen Acronis-Komponenten über das Netzwerk zu starten.

Booten über das Netzwerk:

- Eliminiert die Notwendigkeit eines Technikers vor Ort, um das bootfähige Medium (S. 487) in das zu bootende System einzulegen
- Reduziert bei Gruppen-Operationen die zum Booten mehrerer Maschinen benötigte Zeit (im Vergleich zu physikalischen Bootmedien)

1.4.7.5 License Server

Der Server ermöglicht Ihnen, Lizenzen von Acronis-Produkten zu verwalten und Komponenten, die Lizenzen benötigen, zu installieren.

Sie können einen License Server als separate Komponenten installieren oder den im Management Server integrierten verwenden. Die Funktionalität des License Servers (S. 426) ist für beide Installationsvarianten ähnlich.

1.4.8 Management Konsole

Die Acronis Backup & Recovery 11.5 Management Console ist ein administratives Werkzeug zum Remote- und lokalen Zugriff auf die Acronis Backup & Recovery 11.5 Agenten sowie auf den Acronis Backup & Recovery 11.5 Management Server, falls die Produkt-Editionen über eine Funktion zur zentralen Verwaltung verfügen.

Die Konsole hat zwei Distributionen: zur Installation in Windows und zur Installation in Linux. Obwohl beide Distributionen eine Verbindung zu jedem Acronis Backup & Recovery 11.5 Agenten und Acronis Backup & Recovery 11.5 Management Server ermöglichen, wird empfohlen, die Konsole für Windows zu verwenden, wenn diese Möglichkeit besteht. Die unter Linux installierte Konsole ist in ihrer Funktionalität eingeschränkt:

- Eine Remote-Installation von Acronis Backup & Recovery 11.5-Komponenten ist nicht verfügbar.
- Active Directory-bezogene Funktionen, wie beispielsweise das Durchsuchen des ADs, sind nicht verfügbar.

1.4.9 Bootable Media Builder

Der Acronis Bootable Media Builder ist ein spezielles Werkzeug zur Erstellung bootfähiger Medien (S. 487). Es gibt zwei Media Builder-Distributionen: zur Installation in Windows und zur Installation in Linux.

Der auf Windows installierte Media Builder kann bootfähige Medien schaffen, die entweder auf Windows Preinstallation Environment (WinPE) oder einem Linux-Kernel basieren. Der unter Linux installierte Media Builder erstellt bootfähige Medien, die auf dem Linux-Kernel basieren.

Das Add-on für Universal Restore (S. 15) ermöglicht die Erstellung eines bootfähigen Mediums, das die Fähigkeit zur Wiederherstellung auf abweichender Hardware bietet. Universal Restore handhabt Abweichungen bei Geräten, die kritisch für den Betriebssystemstart sind, wie beispielsweise Speicher-Controller, Hauptplatine oder Chipsatz.

Das Add-on für Deduplizierung (S. 15) ermöglicht Ihnen die Erstellung bootfähiger Medien, die Backups auf deduplizierende Depots erstellen können. Dieses Add-on kann als Erweiterung für beide Media Builder-Distributionen installiert werden.

1.4.10 Acronis Wake-on-LAN Proxy

Der Acronis Wake-on-LAN Proxy ermöglicht es dem Acronis Backup & Recovery 11.5 Management Server, Maschinen eines anderen Subnetzes zur Backup-Durchführung einzuschalten. Der Acronis Wake-on-LAN Proxy kann auf jedem Server im Subnetz installiert werden, auf dem sich die Maschinen befinden, die Sie sichern möchten.

1.5 Über die Verwendung des Produktes im Testmodus

Bevor Sie eine Lizenz von Acronis Backup & Recovery 11.5 kaufen, möchten Sie die Software möglicherweise testen. Dies kann ohne einen Lizenzschlüssel getan werden.

Führen Sie zur Installation des Produktes im Testmodus das Setup-Programm lokal aus oder verwenden Sie die Möglichkeit zur Remote-Installation. Eine unbeaufsichtigte Installation oder andere Installationsvarianten werden nicht unterstützt.

Beschränkungen des Testmodus

Wenn Acronis Backup & Recovery 11.5 im Testmodus installiert wurde, hat es folgende Beschränkungen:

- Die Funktion 'Universal Restore' ist deaktiviert.

Zusätzliche Beschränkungen für bootfähige Medien:

- Die Funktion zur Laufwerksverwaltung ist nicht verfügbar. Sie können alles innerhalb der Benutzeroberfläche testen, aber die Option zur Umsetzung ausstehender Aktionen ist nicht verfügbar.
- Die Recovery-Funktion ist verfügbar, jedoch keine Backup-Funktion. Installieren Sie die Software im Betriebssystem, um auch die Backup-Funktion testen zu können.

Upgrade auf die Vollversion

Nach Ablauf des Testzeitraums wird auf der Benutzeroberfläche des Produkts eine Meldung angezeigt, die Sie dazu auffordert, einen Lizenzschlüssel zu spezifizieren oder zu erwerben.

Um einen Lizenzschlüssel spezifizieren zu können, müssen Sie auf **Hilfe** –> **Lizenz wechseln** (S. 375) klicken. Es ist nicht möglich, den Schlüssel durch Ausführung des Setup-Programms zu spezifizieren.

Falls Sie ein Test- oder Kaufabonnement für den Online Backup Service (S. 460) aktiviert haben, steht Ihnen die Online Backup-Funktion bis zum Ende des Abonnementzeitraums zur Verfügung – unabhängig davon, ob Sie einen Lizenzschlüssel spezifizieren.

1.6 Unterstützte Dateisysteme

Acronis Backup & Recovery 11.5 kann Backups und Wiederherstellungen der folgenden Dateisysteme mit den angegebenen Einschränkungen ausführen:

- FAT16/32
- NTFS
- ReFS – Volume-Recovery ohne die Möglichkeit, die Größe des Volumes zu ändern. Wird nur in Windows Server 2012/2012 R2 (S. 54) unterstützt.
- Ext2/Ext3/Ext4
- ReiserFS3 – aus Laufwerk-Backups, die sich auf dem Acronis Backup & Recovery 11.5 Storage Node befinden, können keine einzelnen Dateien wiederhergestellt werden
- ReiserFS4 – Volume-Wiederherstellung ohne Größenanpassung des Volumes; aus Laufwerk-Backups, die sich auf dem Storage Node in Acronis Backup & Recovery 11.5 befinden, können keine einzelnen Dateien wiederhergestellt werden
- XFS – Volume-Wiederherstellung ohne Größenanpassung des Volumes; aus Disk-Backups, die sich auf dem Storage Node in Acronis Backup & Recovery 11.5 befinden, können keine einzelnen Dateien wiederhergestellt werden
- JFS – aus Laufwerk-Backups, die sich auf dem Acronis Backup & Recovery 11.5 Storage Node befinden, können keine einzelnen Dateien wiederhergestellt werden
- Linux SWAP

Acronis Backup & Recovery 11.5 kann unter Verwendung eines Sektor-für-Sektor-Ansatzes Backups und Wiederherstellungen bei beschädigten oder nicht unterstützten Dateisystemen ausführen.

1.7 Technischer Support

Maintenance- und Support-Programm

Wenn Sie Unterstützung für Ihr Acronis-Produkt benötigen, besuchen Sie http://www.acronis.de/support

Produkt-Updates

Sie können für all Ihre registrierten Acronis-Software-Produkte jederzeit Updates von unserer Website herunterladen, nachdem Sie sich unter **Mein Konto** (http://www.acronis.de/my) eingeloggt und Ihr Programm registriert haben. Weitere Informationen auch in den (englischsprachigen) Artikel unter **Registering Acronis Products at the Website** (http://kb.acronis.com/content/4834) und **Acronis Website User Guide** (http://kb.acronis.com/content/8128).

2 Erste Schritte

 **Schritt 1: Installation**

Diese kurze Installationsanleitung ermöglicht Ihnen, schnell mit der Verwendung des Programms zu beginnen. Zu einer kompletten Beschreibung der Installationsmethoden und Prozeduren siehe die 'Installationsanleitung'.

Stellen Sie vor der Installation Folgendes sicher:

- Ihre Hardware die Systemanforderungen erfüllt.
- Sie für die Edition Ihrer Wahl die entsprechenden Lizenzschlüssel haben.
- Sie haben das Setup-Programm. Sie können es von der Acronis-Website herunterladen.

Vorgehensweise

Wenn Sie den unteren Anweisungen folgen, können Sie der Maschine mehr als eine Funktion zuweisen.

1. Installieren Sie den Management Server, damit Sie mehrere Maschinen verwalten können.
   a. Führen Sie das Setup-Programm aus und klicken Sie auf **Installation von Acronis Backup & Recovery 11.5**.
   b. Aktivieren Sie nach Bestätigung der Lizenzvereinbarung das Kontrollkästchen **Die Sicherung physikalischer und virtueller Maschinen zentral überwachen und konfigurieren**.
   c. Geben Sie Ihre Lizenzschlüssel ein oder importieren Sie diese aus einer Textdatei.
   d. Folgen Sie den Bildschirmanweisungen.

   Details: Auch die Konsole wird installiert, so dass Sie den Management Server lokal steuern können.
2. Installieren Sie auf jeder Maschine, die Sie per Backup sichern wollen, einen Agenten.
   a. Führen Sie das Setup-Programm aus und klicken Sie auf **Installation von Acronis Backup & Recovery 11.5**.
   b. Aktivieren Sie nach Bestätigung der Lizenzvereinbarung das Kontrollkästchen **Daten dieser Maschine sichern**.
   c. Wählen Sie **Ich habe eine Lizenz oder ein Abonnement gekauft**.
   d. Klicken Sie auf **Lizenzen hinzufügen**, aktivieren Sie das Kontrollkästchen **Folgenden License Server verwenden** und geben Sie dann den Namen oder die IP-Adresse des zuvor installierten Management Servers an.
   e. Registrieren Sie auf Nachfrage die Maschinen auf dem Management Server.
   f. Folgen Sie den Bildschirmanweisungen.

   Details: Die Konsole wird zudem auch auf jeder Maschine installiert.
3. [Optional] Installieren Sie den Storage Node auf der Maschine, die als Storage für die Backups anderer Maschinen dienen soll.
   a. Führen Sie das Setup-Programm aus und klicken Sie auf **Installation von Acronis Backup & Recovery 11.5**.
   b. Aktivieren Sie nach Bestätigung der Lizenzvereinbarung das Kontrollkästchen **Backups anderer Maschinen auf dieser Maschine sichern**.
   c. Registrieren Sie auf Nachfrage den Storage Node auf dem Management Server.

   d. Folgen Sie den Bildschirmanweisungen.

4. [Optional] Installieren Sie die Konsole auf einer Maschine, von der aus Sie arbeiten wollen – sofern diese Maschine nicht der Management Server ist und keinen Agenten hat.
   a. Führen Sie das Setup-Programm aus und klicken Sie auf **Installation von Acronis Backup & Recovery 11.5**.
   b. Aktivieren Sie nach Bestätigung der Lizenzvereinbarung das Kontrollkästchen **Verbindung mit Remote Maschinen**.
   c. Folgen Sie den Bildschirmanweisungen.



Schritt 2: Ausführung

Führen Sie die Acronis Backup & Recovery 11.5 Management Console aus.

- In **Windows** — Starten Sie die Konsole, indem Sie **Acronis Backup & Recovery 11.5** aus dem **Start**-Menü auswählen.
- In **Linux** — Melden Sie sich als 'root' oder als normaler Benutzer an und wechseln Sie denn bei Bedarf den Benutzer. Starten Sie die Konsole mit dem Befehl

```
/usr/sbin/acronis_console
```

Informationen zu den Elementen der grafischen Benutzeroberfläche finden Sie unter 'Management Konsole verwenden (S. 25)'.



Schritt 3: Bootfähige Medien

Erstellen Sie ein bootfähiges Medium, damit Sie ein (nicht mehr startfähiges) Betriebssystem wiederherstellen oder auf fabrikneuer Hardware bereitstellen können.

1. Wählen Sie **Werkzeuge –> Bootfähiges Medium erstellen** aus dem Menü.
2. Klicken Sie in der Willkommenseite auf **Weiter**. Klicken Sie solange auf **Weiter**, bis die Liste der Komponenten erscheint.
3. Fahren Sie wie im Abschnitt 'Linux-basiertes bootfähiges Medium (S. 285)' beschrieben fort.



Schritt 4: Verbindung

Verbinden Sie die Konsole mit dem Management Server oder einer verwalteten Maschine.

Klicken Sie auf der ersten Seite der Konsole auf einen der folgenden Befehle:



Diese Maschine verwalten
Falls der Agent auf derselben Maschine wie die Konsole installiert ist.



Remote-Maschine verwalten
Falls der Agent auf einer Remote-Maschine installiert ist.



Zu einem Management Server verbinden
Zur Verwaltung mehrerer physikalischer und virtueller Maschinen.



Schritt 5: Backup



Backup jetzt (S. 58)

Klicken Sie auf **Backup jetzt**, um ein einmaliges Backup mit wenigen, einfachen Schritten durchzuführen. Der Backup-Prozess wird unmittelbar ausgeführt, sobald Sie alle benötigten Schritte durchgeführt haben.

So speichern Sie Ihre Maschine in eine Datei:

Klicken Sie unter **Backup-Ziel** auf **Speicherort** und wählen Sie dann, wo das Backup gespeichert werden soll. Klicken Sie auf **OK**, um Ihre Auswahl zu bestätigen. Klicken Sie im unteren Fensterbereich auf **OK**, um das Backup zu starten.

Tipp: Durch Verwendung eines bootfähigen Mediums können Sie Offline-Backups ('kalte' Backups) auf dieselbe Art erstellen wie im Betriebssystem.



Backup-Plan erstellen (S. 58)

Erstellen Sie einen Backup-Plan, falls Sie eine langfristige Backup-Strategie benötigen, die Backup-Schema sowie Planungen und Bedingungen einschließt, um Backups zeitabhängig zu löschen oder sie an andere Orte zu verschieben.

Hinweise für Benutzer der Advanced-Editionen: Wenn Sie einen Backup-Plan auf dem Management Server erstellen, dann können Sie:

– Komplette Maschinen oder Maschinengruppen wählen.

– Unterschiedliche Datenelemente auf jeder Maschine wählen.

– Auswahlregeln verwenden, um dieselben Datenelemente auf unterschiedlichen Maschinen zu wählen.

Auf diese Art erstellen Sie einen zentralen Backup-Plan, der auf den gewählten Maschinen bereitgestellt wird. Weitere Informationen finden Sie bei 'Erstellung eines zentralen Backup-Plans (S. 396)'.



Schritte 6: Recovery



Recovery (S. 146)

Sie müssen für eine Wiederherstellung die im Backup gesicherten Daten wählen – sowie den Zielort, an dem die Daten wiederhergestellt werden sollen. Als Ergebnis dieser Aktion wird ein Recovery-Task erstellt.

Die Wiederherstellung eines Laufwerks bzw. Volumes über ein Volume, welches durch das Betriebssystem gesperrt ist, erfordert einen Neustart. Nach dem Abschluss der Wiederherstellung geht das wiederhergestellte Betriebssystem automatisch online.

Sollte eine Maschine nicht mehr booten können oder Sie ein System auf fabrikneue Hardware wiederherstellen müssen, dann booten Sie die Maschine mit einem bootfähigen Medium und konfigurieren Sie dort die Wiederherstellungsaktion auf die gleiche Art wie den Recovery-Task.

Hinweise für Benutzer der Advanced-Editionen: Sie können Aktionen unter einem bootfähigen Medium nicht mit dem Management Server steuern. Aber Sie können die Verbindung der Konsole zum Server trennen und sie mit der Maschine verbinden, die mit dem Medium gebootet wurde.



Schritt 7: Verwaltung

Der Fensterbereich **Navigation** (im linken Bereich der Konsole) ermöglicht Ihnen, zwischen den Produktansichten zu navigieren, die verschiedenen administrativen Zwecken dienen.

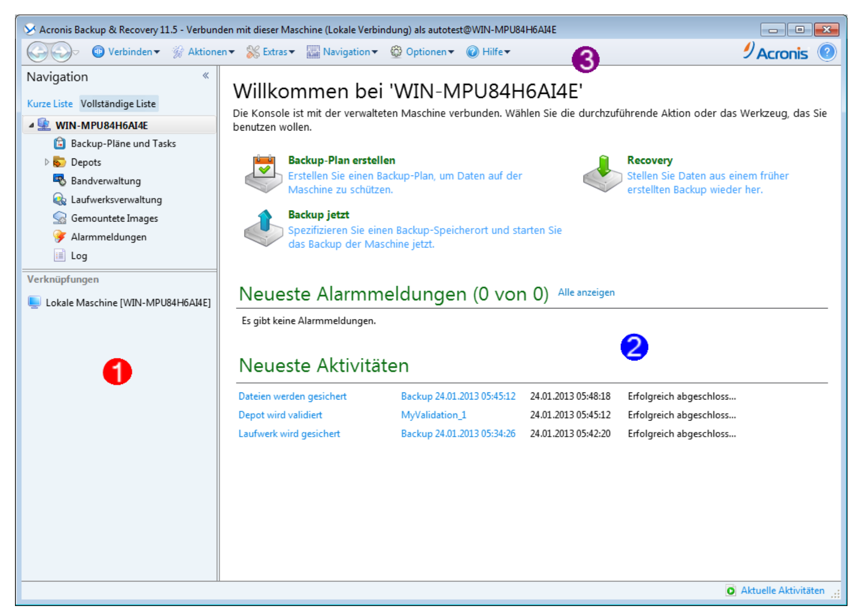
- Verwenden Sie die Anzeige **Backup-Pläne und Tasks**, um Backup-Pläne und Tasks zu verwalten: Sie können hier Tasks ausführen, bearbeiten, stoppen und löschen sowie ihre Stadien und ihren Fortschritt einsehen.
- Verwenden Sie die Anzeige **Alarmmeldungen**, um Probleme schnell erkennen und lösen zu können.
- Verwenden Sie die Anzeige **Logs**, um die Ereignismeldungen von Aktionen einzusehen.
- Der Ort, an dem Sie Ihre Backup-Dateien speichern, wird Depot (S. 489) genannt. Wechseln Sie zur Anzeige **Depots** (S. 201), um Informationen über Ihre Depots zu erhalten. Navigieren Sie von dort aus weiter zu dem gewünschten Depot, um Backups und ihre Inhalte einzusehen. Sie können Daten für eine Wiederherstellung auswählen und diverse manuelle Aktionen mit Backups durchführen (mounten, validieren, löschen etc.).

Management Server administrieren

- Verwenden Sie die Anzeige **Maschinen mit Agenten**, um auf dem Management Server registrierte Maschinen zu verwalten. Um mit einer großen Anzahl von Maschinen effektiver arbeiten zu können, können Sie sie in Gruppen (S. 408) organisieren.
- Verwenden Sie die Anzeige **Virtuelle Maschinen** (S. 422), um unterstützte Virtualisierungsumgebungen zu verwalten.
- Wenn Sie sich dafür entscheiden, alle Backup-Archive an einem oder wenigen Netzwerkorten zu speichern, dann erstellen Sie zentrale Depots an diesen Speicherorten. Nachdem Sie ein Depot erstellt haben, können Sie seinen Inhalt einsehen und verwalten. Wählen Sie dazu im Fensterbereich **Navigation** die Elemente **Depots –>** **Zentral –>** **'Depot-Name'** . Die Verknüpfung zum Depot wird an alle registrierten Maschinen verteilt. Das Depot kann in jedem von Ihnen oder anderen Benutzern der registrierten Maschinen erstellten Backup-Plan als Zielspeicherort für das Backup angegeben werden.
- Erstellen Sie zentral verwaltete Depots auf dem Storage Node (S. 248), um Folgendes tun zu können:
  - Den **Datenkatalog** (S. 150) nach einer gewünschten Version von Backup-Daten in allen verwalteten Depots durchsuchen.
  - Die Backups mehrerer Maschinen auf Bandgeräte (S. 223) sichern, die an den Storage Node angeschlossen sind.
  - Deduplizierung (S. 259) verwenden, um den durch die Daten belegten Speicherplatz zu minimieren und die Netzwerkbelastung während der Backup-Erstellung zu verringern.

2.1 Die Management Konsole verwenden

Sobald die Konsole mit einer verwalteten Maschine (S. 496) oder einem Management Server (S. 493) verbunden ist, werden die entsprechenden Elemente in der gesamten Arbeitsumgebung der Konsole angezeigt (im Menü, im Hauptbereich mit der **Willkommensseite** oder im Fensterbereich **Navigation**), wodurch Ihnen ermöglicht wird, agenten- oder serverspezifische Aktionen durchzuführen.



Acronis Backup & Recovery 11.5 Management Console – Willkommensseite

Wichtige Elemente der Arbeitsfläche der Konsole

	Name	Beschreibung
1	Fensterbereich **Navigation**	Enthält den Verzeichnisbaum **Navigation** und den Bereich **Verknüpfungen**. Ermöglicht Ihnen eine Navigation zwischen unterschiedlichen Ansichten. Weitere Informationen finden Sie unter Fensterbereich 'Navigation' (S. 26).
2	Hauptbereich	Sie können hier Backup-, Recovery- und andere Aktionen konfigurieren und überwachen. Die im Hauptbereich angezeigten Ansichten und Aktionsseiten (S. 28) hängen von den Elementen ab, die im Menü oder Verzeichnisbaum **Navigation** ausgewählt wurden.
3	**Menüleiste**	Wird quer über den oberen Bereich des Programmfensters angezeigt. Ermöglicht Ihnen, die gängigsten Aktionen von Acronis Backup & Recovery 11.5 auszuführen. Die Menüelemente ändern sich dynamisch, abhängig vom im Verzeichnisbaum **Navigation** und im Hauptbereich ausgewählten Element.

2.1.1 Fensterbereich 'Navigation'

Der Fensterbereich 'Navigation' enthält den Verzeichnisbaum **Navigation** und den Bereich **Verknüpfungen**.

Verzeichnisbaum 'Navigation'

Mit Hilfe des Verzeichnisbaums **Navigation** können Sie sich durch die Programmansichten bewegen. Welche Ansichten verfügbar sind, hängt davon ab, ob die Konsole mit einer verwalteten Maschine oder mit dem Management Server verbunden ist. In beiden Fällen können für die Ansichten zwischen der **Vollständigen Liste** oder der **Kurzen Liste** wählen. Die **Kurze Liste** enthält die am häufigsten verwendeten Ansichten der **Vollständigen Liste**.

Ansichten für eine verwaltete Maschine

Wenn die Konsole mit einer verwalteten Maschine verbunden ist, sind die folgenden Ansichten im Verzeichnisbaum 'Navigation' verfügbar.

Die Anzeige der **Kurzen Liste** enthält

- **[Name der Maschine]**. Die oberste Ebene des Verzeichnisbaums, auch **Willkommenseite** genannt. Hier wird der Name der Maschine angezeigt, mit der die Konsole momentan verbunden ist. Verwenden Sie diese Ansicht, um schnell auf wichtige Aktionen zuzugreifen, die auf der verwalteten Maschine verfügbar sind.
  - **Backup-Pläne und Tasks**. Verwenden Sie diese Ansicht, um Backup-Pläne und Tasks auf der verwalteten Maschine zu verwalten: Sie können Tasks hier ausführen, bearbeiten, stoppen und löschen sowie ihren Fortschritt einsehen.
  - **Depots**. Verwenden Sie diese Ansicht, um persönliche Depots und darin gespeicherte Archive zu verwalten, neue Depots hinzuzufügen, bestehende Depots umzubenennen oder zu löschen, Depots zu validieren, Backup-Inhalte zu untersuchen usw. Falls die Maschine auf dem Management Server registriert ist, können Sie die zentralen Depots durchsuchen und Aktionen mit solchen Archiven durchführen, für die Sie die entsprechenden Berechtigungen haben.
  - **Alarmmeldungen**. Verwenden Sie diese Ansicht, um Warnmeldungen für die verwaltete Maschine zu untersuchen.

Die Anzeige der **Vollständigen Liste** enthält zusätzlich

  - **Bandverwaltung**. Verwenden Sie diese Ansicht, um Aktionen mit Bändern auszuführen.
  - **Laufwerksverwaltung**. Verwenden Sie diese Ansicht, um Aktionen mit den Festplatten und ähnlichen Laufwerken einer Maschine auszuführen.
  - **Log**. Verwenden Sie diese Ansicht, um Informationen zu solchen Aktionen zu überprüfen, die vom Programm auf der verwalteten Maschine ausgeführt werden.
  - **Gemountete Images**. Dieser Knoten wird angezeigt, wenn mindestens ein Volume gemountet ist. Verwenden Sie diese Ansicht, um gemountete Images zu verwalten.

Ansichten für einen Management Server

Wenn die Konsole mit einem Management Server verbunden ist, sind die folgenden Ansichten im Verzeichnisbaum 'Navigation' verfügbar.

Die Anzeige der **Kurzen Liste** enthält

- **[Name des Management Servers]**. Die oberste Ebene des Verzeichnisbaums, auch **Willkommenseite** genannt. Hier wird der Name des Management Servers angezeigt, mit dem die Konsole momentan verbunden ist. Verwenden Sie diese Ansicht, um schnell auf wichtige Aktionen zuzugreifen, die auf dem Management Server verfügbar sind.
  - **Dashboard**. Verwenden Sie diese Ansicht, um auf einen Blick einschätzen zu können, ob die Daten auf den beim Management Server registrierten Maschinen erfolgreich gesichert sind.
  - **Maschinen mit Agenten**. Verwenden Sie diese Ansicht, um auf dem Management Server registrierte Maschinen zu verwalten.
  - **Backup-Pläne und Tasks**. Verwenden Sie diese Ansicht, um zentrale Backup-Pläne und Tasks auf dem Management Server zu verwalten.
  - **Depots**. Verwenden Sie diese Ansicht, um zentrale Depots und darin gespeicherte Archive zu verwalten: Sie können neue, zentrale Depots erstellen, bestehende Depots umbenennen oder löschen, Depot-Benutzer und Administratoren zuweisen, Aktionen auf Archive und Backups anwenden usw.
  - **Alarmmeldungen**. Verwenden Sie diese Ansicht, um Warnmeldungen für den Management Server und alle registrierten Maschinen zu untersuchen.

Die Anzeige der **Vollständigen Liste** enthält zusätzlich

- **Datenkatalog**. Verwenden Sie diese Ansicht, um schnell nach einer benötigten Version von gesicherten Daten in dem zentral verwalteten Depots zu suchen.
- **Virtuelle Maschinen**. Verwenden Sie diese Ansicht, um unterstützte Virtualisierungsumgebungen zu verwalten.
- **Storage Nodes**. Verwenden Sie diese Ansicht, um Storage Nodes zu verwalten. Sie können hier einen Storage Node hinzufügen, damit Sie zentrale Depots erstellen können, die vom Knoten verwaltet werden.
- **Bandverwaltung**. Verwenden Sie diese Ansicht, um Aktionen mit Bändern auszuführen.
- **Lizenzen**. Verwenden Sie diese Ansicht, um Lizenzen zu verwalten.
- **Berichte**. Verwenden Sie diese Ansicht, um Berichte zu generieren.
- **Log**. Verwenden Sie diese Ansicht, um den Verlauf von zentralen Verwaltungsaktionen zu untersuchen – oder den Verlauf von aufgezeichneten Aktionen in den lokalen Logs der registrierten Maschinen und der Storage Nodes.

Seitenleistenbereich 'Verknüpfungen'

Der Bereich **Verknüpfungen** wird unterhalb des Verzeichnisbaums 'Navigation' angezeigt. Ermöglicht Ihnen, in einfacher und bequemer Weise eine Verbindung mit oft benötigten Maschinen herzustellen, indem Sie diese als Shortcuts hinzufügen.

So weisen Sie einer Maschine eine Verknüpfung zu

1. Verbinden Sie die Konsole mit einer verwalteten Maschine.
2. Klicken Sie im Verzeichnisbaum 'Navigation' mit der rechten Maustaste auf den Namen der Maschine (Stammelement des Verzeichnisbaums 'Navigation') und wählen Sie **Verknüpfung erstellen**.

   Wenn die Konsole und der Agent auf derselben Maschine installiert sind, wird die Verknüpfung auf diese Maschine automatisch als **Lokale Maschine [Name der Maschine]** zum Bereich 'Verknüpfungen' hinzugefügt.

Aktionen mit den seitlichen Fensterbereichen

So erweitern/minimieren Sie Fensterbereiche

Der Fensterbereich **Navigation** erscheint standardmäßig erweitert. Möglicherweise müssen Sie den Fensterbereich minimieren, um sich zusätzliche freie Arbeitsfläche zu verschaffen. Klicken Sie dazu auf das entsprechende Chevron-Symbol (). Der Fensterbereich wird daraufhin minimiert und das Chevron-Symbol ändert seine Orientierung (). Klicken Sie ein weiteres Mal auf das Chevron-Symbol, um den Fensterbereich zu erweitern.

So ändern Sie die Begrenzungen der Fensterbereiche.

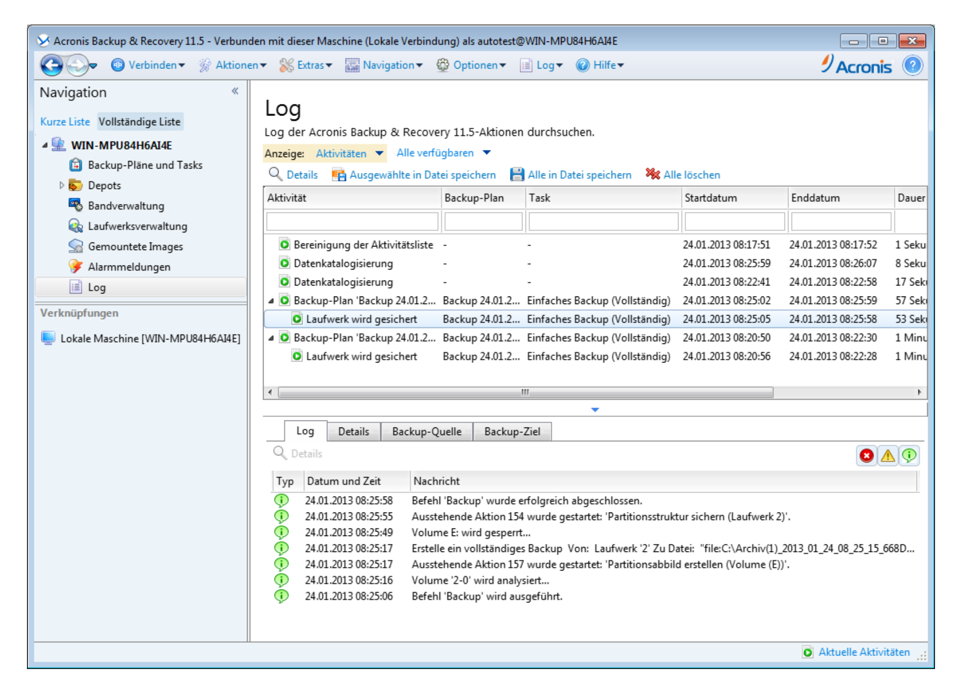
1. Zeigen Sie auf die Begrenzungslinie des Fensterbereiches.
2. Wenn der Zeiger als Pfeil mit zwei Spitzen angezeigt wird, dann ziehen Sie, um den Rand zu verschieben.

2.1.2 Hauptfenster, Ansichten und Aktionsseiten

Das Hauptfenster ist der zentrale Bereich, in dem Sie mit der Konsole arbeiten. Sie können Backup-Pläne und Recovery-Tasks erstellen, bearbeiten und verwalten sowie andere Aktionen ausführen. Die im Hauptbereich angezeigten Ansichten und Aktionsseiten hängen von den Elementen ab, die Sie im Menü oder im Verzeichnisbaum **Navigation** auswählen.

2.1.2.1 Ansichten

Wenn Sie auf ein beliebiges Element im **Navigationsbaum** der Seitenleiste Navigation (S. 26) klicken, wird eine entsprechende Ansicht angezeigt.



Ansicht „Log“

Übliche Arbeitsweise mit Ansichten

In der Regel enthält jede Ansicht eine Tabelle mit Elementen, eine Symbolleiste mit Schaltflächen für die Tabelle sowie den unteren Fensterbereich **Informationen**.

- Verwenden Sie die Funktionen zum Filtern und Sortieren (S. 29), um die Tabelle nach dem gewünschten Element zu durchsuchen.
- Wählen Sie in der Tabelle das gewünschte Element aus.
- Sehen Sie sich im Fensterbereich Informationen (standardmäßig eingeklappt) die Details des Elements an. Sie können den Fensterbereich aufklappen, indem Sie auf das Pfeilsymbol klicken.
- Führen Sie die entsprechenden Aktionen mit dem ausgewählten Element aus. Es gibt verschiedene Möglichkeiten, wie Sie ein und dieselbe Aktion mit ausgewählten Elementen ausführen können:
  - Indem Sie auf die Schaltflächen in der Symbolleiste der Tabelle klicken.
  - Indem Sie die Elemente im Menü **Aktionen** wählen.
  - Indem Sie mit der rechten Maustaste auf das Element klicken und die Aktion im Kontextmenü auswählen.

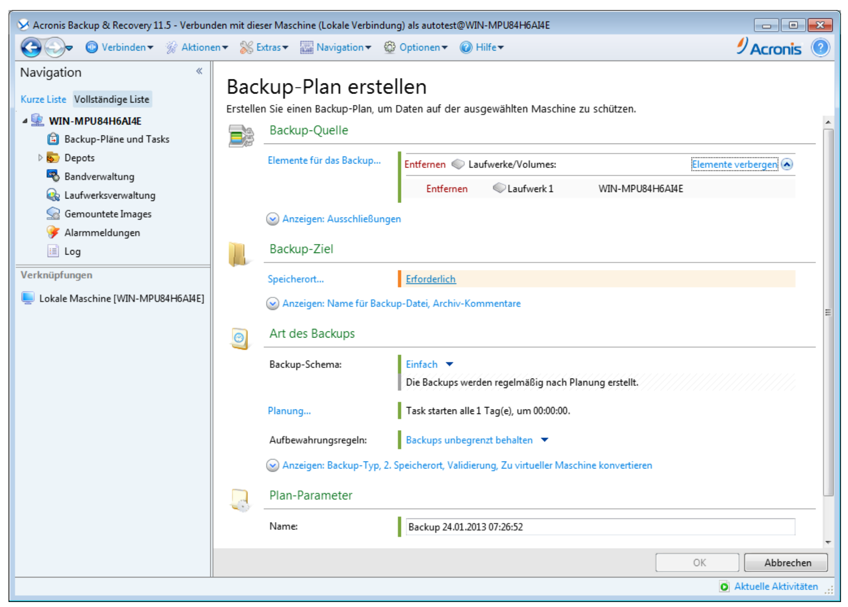
Tabellenelemente sortieren, filtern und konfigurieren

Nachfolgend finden Sie eine Anleitung, wie Sie Tabellenelemente in jeder Ansicht sortieren, filtern und konfigurieren können.

Aufgabe	Tun Sie Folgendes
Elemente nach Spalten sortieren	Klicken Sie auf einen Spaltenkopf, um die Elemente aufsteigend sortieren zu lassen. Kicken Sie erneut auf den Spaltenkopf, um die Elemente in absteigender Reihenfolge sortieren zu lassen.
Elemente nach einem vordefinierten Spaltenwert filtern	Wählen Sie in einem Feld unter der entsprechenden Spaltenkopf den gewünschten Wert aus dem Listenfeld.
Elemente nach einem eingegebenen Wert filtern	Geben Sie in einem Feld unter dem entsprechenden Spaltenkopf einen Wert ein. Als Ergebnis sehen Sie eine Liste von Werten, die vollständig oder teilweise mit dem eingegebenen Wert übereinstimmen.
Elemente nach vordefinierten Parametern filtern	Klicken Sie auf die entsprechenden Schaltflächen über der Tabelle. Sie können beispielsweise in der Ansicht **Log** die Log-Einträge nach dem Ereignistyp filtern (Information, Warnung, Fehler) oder nach dem Zeitraum, in dem das Ereignis auftrat (**Der letzten 24 Stunden**, **Der letzten Woche**, **Der letzten 3 Monate** oder **Benutzerdefinierter Zeitraum**).
Tabellenspalten anzeigen oder verbergen	Standardmäßig hat jede Tabelle eine bestimmte Anzahl von angezeigten Spalten, während andere verborgen sind. Sie können nicht benötigte Spalten außerdem ausblenden bzw. ausgeblendete anzeigen lassen. Spalten anzeigen oder verbergen 1. Klicken Sie mit der rechten Maustaste auf einen Spaltenkopf, um das Kontextmenü zu öffnen. 2. Klicken Sie auf die Elemente, die Sie anzeigen bzw. verbergen wollen.

2.1.2.2 Aktionsseiten

Wenn Sie im Menü **Aktionen** auf ein Element klicken, erscheint im Hauptbereich eine Aktionsseite. Diese enthält Schritte, die Sie ausführen müssen, um einen beliebigen Task oder einen Backup-Plan zu erstellen und zu starten.



Aktionsseite – Backup-Plan erstellen

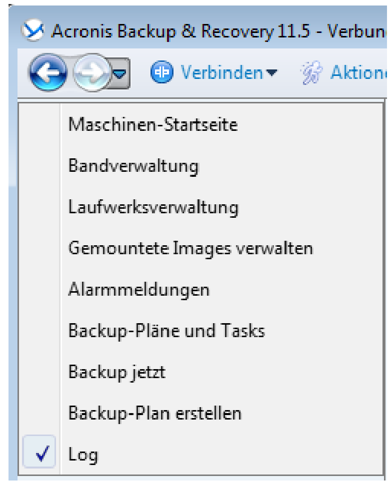
Steuerelemente verwenden und Einstellungen festlegen

Verwenden Sie die aktiven Steuerelemente, um die Einstellungen und Parameter eines Backup-Plans oder Recovery-Tasks zu spezifizieren. Standardmäßig handelt es sich bei diesen Feldern um Anmeldedaten, Optionen, Kommentare und einige andere, verborgene. Die meisten Einstellungen werden konfiguriert, indem Sie auf die entsprechenden Links **Anzeigen...** klicken. Andere Einstellungen werden aus einem Listenfeld ausgewählt oder manuell in die Felder auf der Seite eingegeben.



Aktionsseite – Steuerelemente

Acronis Backup & Recovery 11.5 merkt sich die Änderungen, die Sie auf den Aktionsseiten vornehmen. Wenn Sie z.B. begonnen haben, einen Backup-Plan zu erstellen und dann aus irgendeinem Grund zu einer anderen Ansicht gewechselt sind, ohne die Plan-Erstellung abzuschließen, können Sie die Navigationsschaltfläche **Zurück** im Menü anklicken. Oder, wenn Sie bereits mehrere Schritte vorwärts gegangen sind, klicken Sie den Pfeil **Nach unten** und wählen die Seite, auf der Sie die Plan-Erstellung aus der Liste gestartet haben. Auf diese Weise können Sie die verbleibenden Schritte ausführen und die Erstellung des Backup-Plans abschließen.



Navigationsschaltflächen

2.1.3 Konsolen-Optionen

Die Konsolenoptionen legen fest, wie die Informationen in der grafischen Benutzeroberfläche von Acronis Backup & Recovery 11.5 erscheinen.

Um auf die Konsolenoptionen zuzugreifen, wählen Sie **Optionen -> Konsolenoptionen** im Menü.

2.1.3.1 Optionen für Alarmanzeige

Die Option spezifiziert, welche Alarmmeldungen in der Ansicht **Alarmmeldungen** angezeigt bzw. verborgen werden sollen.

Voreinstellung ist: **Alle Alarmmeldungen**.

Um Alarmmeldungen anzuzeigen (zu verbergen), (de)aktivieren Sie die Kontrollkästchen neben den entsprechenden Alarmtypen.

2.1.3.2 Anmeldedaten zwischenspeichern

Diese Option spezifiziert, ob die bei Verwendung der Management Konsole eingegebenen Anmeldedaten gespeichert werden sollen.

Voreinstellung ist: **Aktiviert**.

Ist die Option aktiviert, dann werden die von Ihnen während einer Konsolensitzung für verschiedene Speicherorte eingegebenen Anmeldedaten zur Nutzung in späteren Sitzungen gespeichert. Unter Windows werden die Anmeldedaten in der Anmeldeinformationsverwaltung (Windows Credentials Manager) gespeichert. Unter Linux werden die Anmeldedaten in einer speziellen, verschlüsselten Datei gespeichert.

Ist die Option deaktiviert, dann werden die Anmeldedaten nur solange zwischengespeichert, bis die Konsole geschlossen wird.

Um die für das aktuelle Benutzerkonto zwischengespeicherten Anmeldedaten zu löschen, klicken Sie auf die Schaltfläche **Cache für Anmeldedaten bereinigen**.

2.1.3.3 Schriftarten

Die Option legt fest, welche Schriftarten in der grafischen Benutzeroberfläche von Acronis Backup & Recovery 11.5 erscheinen. Die Einstellung **Menü-Schriftart** beeinflusst die Dropdown- und Kontextmenüs. Die Einstellung **Anwendung-Schriftart** beeinflusst alle anderen Benutzeroberflächenelemente.

Voreinstellung ist: **Systemstandardschriftart** sowohl für die Menüs als für die Schnittstellenelemente der Anwendung.

Um eine Auswahl zu treffen, wählen Sie die Schriftart im jeweiligen Listenfeld und stellen die Schrifteigenschaften ein. Sie können eine Vorschau der Schriftenanzeige erhalten, wenn Sie rechts daneben auf **Durchsuchen** klicken.

2.1.3.4 Pop-up-Meldungen

Diese Optionen sind wirksam, wenn die Konsole mit einer verwalteten Maschine oder mit dem Management Server verbunden ist.

Der Dialog 'Aktivitäten, die einen Benutzereingriff erfordern'

Diese Option legt fest, ob ein Pop-up-Fenster angezeigt werden soll, wenn ein oder mehrere Aktivitäten einen Benutzereingriff erfordern. Dieses Fenster ermöglicht Ihnen, für alle Aktivitäten eine Entscheidung zu spezifizieren, beispielsweise ob einen Neustart bestätigt werden soll oder ob nach Freigabe von Speicherplatz eine Aktion wiederholt werden soll. So lange wenigstens eine Aktivität einen Benutzereingriff erfordert, können Sie dieses Fenster jederzeit von der Willkommensseite der verwalteten Maschine aus öffnen. Alternativ können Sie die Ausführungsstadien des Tasks in der Ansicht **Backup-Pläne und Tasks** überprüfen und Ihre Entscheidung für jeden Task im Informationsbereich treffen.

Voreinstellung ist: **Aktiviert.**

Um eine Auswahl zu treffen, (de)aktivieren Sie das Kontrollkästchen zum **Dialog 'Aktivitäten, die einen Benutzereingriff erfordern'**.

Der Dialog 'Rückmeldebestätigung'

Diese Option definiert, ob ein Pop-up-Fenster mit Systeminformationen nach Auftreten eines Fehlers angezeigt werden soll. Sie können diese Informationen an den Acronis-Support schicken.

Voreinstellung ist: **Aktiviert.**

Um eine Auswahl zu treffen, (de)aktivieren Sie das Kontrollkästchen zum **Dialog 'Rückmeldebestätigung'**.

Benachrichtigen, wenn kein bootfähiges Medium erstellt wurde

Diese Option definiert, ob ein Pop-up-Fenster angezeigt werden sollen, wenn die Management Konsole auf einer Maschine gestartet wird und auf dieser Maschine bisher noch kein bootfähiges Medium erstellt wurde.

Voreinstellung ist: **Aktiviert.**

(De)Aktivieren Sie zur Auswahl das Kontrollkästchen **Benachrichtigen, wenn kein bootfähiges Medium erstellt wurde**.

Benachrichtigen, wenn die Management Konsole mit einer Komponente einer anderen Version verbunden ist

Diese Option definiert, ob ein Pop-up-Fenster angezeigt werden sollen, wenn eine Konsole mit einem Agenten verbunden ist und sich deren Versionen unterscheiden.

Voreinstellung ist: **Aktiviert.**

Um eine Auswahl zu treffen, müssen Sie das Kontrollkästchen **Benachrichtigen, wenn die Management Konsole mit einer Komponente einer anderen Version verbunden ist** entsprechend (de)aktivieren.

Erfrage Beschreibung bei Auswurf des Bandes

Diese Option definiert, ob eine Benutzeranfrage zur Beschreibung eines Bandes angezeigt werden sollen, wenn Sie es aus einem Bandgerät auswerfen(s.237) lassen, das von Acronis Backup & Recovery 11.5 verwendet wird. Sie können beispielsweise den physikalischen Speicherort beschreiben, wo das Band aufbewahrt wird (empfohlen). Wird ein Band, gemäß der Option **Bänder nach erfolgreichen Backups auswerfen**(s.138)**,** automatisch ausgeworfen, dann erscheint keine solche Benutzereingabeaufforderung.

Voreinstellung ist: **Aktiviert.**

Um eine Auswahl zu treffen, (de)aktivieren Sie das Kontrollkästchen **Erfrage Beschreibung bei Auswurf des Bandes**.

Über Ergebnisse der Task-Ausführung

Die Option legt fest, ob die Pop-up-Meldungen über Ergebnisse der Task-Ausführung erscheinen: Erfolgreiche Vollendung, Fehlschlagen oder erfolgreicher Abschluss mit Warnungen. Wenn die Anzeige der Pop-up-Meldungen deaktiviert ist, können Sie die Ausführungsstadien und Ergebnisse des Tasks in der Ansicht **Backup-Pläne und Tasks** überprüfen.

Voreinstellung ist: **Aktiviert** für alle Ergebnisse.

Um eine Einstellung für jedes Ergebnis ('Erfolgreiche Vollendung', 'Fehlschlagen' oder 'Erfolgreicher Abschluss mit Warnungen') einzeln festzulegen, benutzen Sie das zugehörige Kontrollkästchen.

2.1.3.5 Startseite

Diese Option definiert, ob die **Willkommenseite** oder das **Dashboard** bei Verbindung der Konsole mit dem Management Server angezeigt werden soll.

Voreinstellung ist: die **Willkommenseite**.

Um eine Auswahl zu treffen, (de)aktivieren Sie das Kontrollkästchen **Die Dashboard-Ansicht anzeigen**.

Diese Option kann auch in der **Willkommenseite** gesetzt werden. Wenn Sie das Kontrollkästchen für **Beim Start Dashboard anstelle der aktuellen Ansicht zeigen** in der **Willkommenseite** aktivieren, dann erreichen Sie den gleichen Effekt.

3 Acronis Backup & Recovery 11.5 verstehen

Dieser Abschnitt bemüht sich, den Lesern ein klareres, vertieftes Verständnis des Produktes zu vermitteln, damit es sich auch ohne Schritt-für-Schritt-Anleitungen unter den unterschiedlichsten Umständen erfolgreich einsetzen lässt.

3.1 Besitzer

In diesem Abschnitt wird das Konzept von Backup-Plan-/Task-Besitzern und Archiv-Besitzern erklärt.

Plan- oder Task-Besitzer

Ein lokaler Backup-Plan-Besitzer ist derjenige Benutzer, der den Plan erstellt oder als letzter verändert hat.

Der Besitzer eines zentralen Backup-Plans ist derjenige Management Server-Administrator, der den zentralen Backup-Plan erstellt oder als letzter modifiziert hat.

Tasks, die Bestandteil eines Backup-Plans sind (entweder lokal oder zentral), gehören einem Backup-Plan-Besitzer.

Tasks, die kein Bestandteil eines Backup-Plans sind (wie z.B. Recovery-Tasks), gehören dem Benutzer, der den Task erstellt oder als letzter modifiziert hat.

Einen Plan (Task) verwalten, der einem anderen Benutzer gehört

Ein Benutzer, der auf einer Maschine administrative Berechtigungen hat, kann die lokalen Backup-Pläne und Tasks eines jeden Benutzers, der im Betriebssystem registriert ist, verändern.

Wenn ein Benutzer einen Plan oder Task, der einem anderen Benutzer gehört, zur Bearbeitung öffnet, werden alle in diesem Task gesetzten Passwörter gelöscht. Das verhindert ein Vorgehen „verändere die Einstellungen, behalte Passwörter". Das Programm reagiert jedes Mal mit einer Warnung, wenn Sie versuchen, einen Plan (Task) zu editieren, den zuletzt ein anderer Benutzer modifiziert hat. Wenn Sie die Warnung sehen, haben Sie zwei Möglichkeiten:

- Klicken Sie auf **Abbrechen** und erstellen Sie einen eigenen Plan oder Task. Der ursprüngliche Task bleibt dabei intakt.
- Fahren Sie mit dem Editieren fort. In dem Fall müssen Sie alle zur Ausführung des Plans oder Tasks benötigten Anmeldedaten eingeben.

Archiv-Besitzer

Ein Archiv-Besitzer ist der Benutzer, der das Archiv am Zielort gespeichert hat. Präziser gesagt ist es derjenige Anwender, dessen Konto bei Erstellung des Backup-Plans im Schritt **Backup-Ziel festlegen** angegeben wurde. Standardmäßig werden die Anmeldedaten des Backup-Plans verwendet.

3.2 In Backup-Plänen und Tasks verwendete Anmeldedaten

Dieser Abschnitt erläutert das Konzept von Zugriffsanmeldedaten, Anmeldedaten für Backup-Pläne und Anmeldedaten für Tasks.

Zugriffsanmeldedaten

Sie müssen beim Durchsuchen von Backup-Speicherorten, der Einrichtung von Backups oder der Erstellung von Recovery-Tasks möglicherweise Anmeldedaten bereitstellen, um auf unterschiedliche Ressourcen zugreifen zu können. Ressourcen wie die Daten, die Sie per Backup sichern wollen oder den Speicherort, wo die Backups gespeichert sind (oder gespeichert werden sollen).

Falls die Option **Anmeldedaten zwischenspeichern** (S. 32) aktiviert ist (standardmäßig aktiviert), werden die von Ihnen während einer Konsolensitzung bereitgestellten Anmeldedaten zur Verwendung in späteren Sitzungen gespeichert. Sie müssen die Anmeldedaten daher beim nächsten Mal nicht erneut eingeben. Die Anmeldedaten werden für jeden Besitzer, der die Konsole auf der Maschine verwendet, unabhängig zwischengespeichert.

Anmeldedaten des Backup-Plans

Jeder Backup-Plan, der auf einer Maschine läuft, läuft im Namen eines bestimmten Benutzers.

In Windows:

Der Plan läuft standardmäßig unter dem Konto des Agenten-Dienstes (Agent Service), sofern er durch einen Benutzer erstellt wurde, der auf der Maschine administrative Berechtigungen hat. Falls er durch einen normalen Benutzer erstellt wurde, etwa einem Mitglied der Gruppe **Benutzer**, dann läuft der Plan unter dem Konto dieses Benutzers.

Sie werden bei Erstellung eines Backup-Plans nur in bestimmten Fällen nach Anmeldedaten gefragt. Beispielsweise:

- Sie planen Backups als ein normaler Benutzer und haben bei Verbindung der Konsole mit der Maschine keine Anmeldedaten eingegeben. Dies kann der Fall sein, wenn Sie eine Standalone-Produktedition verwenden oder die Konsole durch Anklicken des Befehls **Diese Maschine verwalten** verbunden haben.
- Sie sichern einen Microsoft Exchange-Cluster per Backup zu einem Storage Node.

Die Anmeldedaten explizit spezifizieren

Sie haben die Möglichkeit, explizit ein bestimmtes Benutzerkonto zu spezifizieren, unter dem der Backup-Plan ausgeführt wird. So gehen Sie auf der Seite zur Backup-Plan-Erstellung vor:

1. Klicken Sie im Bereich **Plan-Parameter** auf **Anmeldedaten des Plans, Kommentare, Bezeichnung anzeigen**.
2. Klicken Sie auf **Anmeldedaten des Plans**.
3. Geben Sie die Anmeldedaten ein, unter denen der Plan laufen soll. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.

In Linux:

Sie müssen keine Anmeldedaten für Backup-Pläne spezifizieren. Unter Linux laufen Backup-Pläne immer unter dem Benutzerkonto 'root'.

Anmeldedaten für den Task

Wie ein Backup-Plan läuft auch jeder Task im Namen eines bestimmten Benutzers.

In Windows:

Beim Erstellen eines Tasks haben Sie die Möglichkeit, explizit ein Konto anzugeben, unter dem der Task laufen wird. Ihre Wahl hängt davon ab, ob die Ausführung des Tasks manuell oder zeit- bzw. ereignisgesteuert erfolgen soll.

- **Manueller Start**

  Jedes Mal, wenn Sie einen Task manuell starten, wird er mit den Anmeldedaten ausgeführt, mit denen Sie zu der Zeit am System angemeldet sind. Außerdem kann der Task auch von jeder Person, die auf der Maschine über administrative Rechte verfügt, gestartet werden. Der Task wird dann unter den Anmeldedaten dieser Person ausgeführt.

  Für den Fall, dass Sie die Anmeldedaten für einen Task explizit spezifizieren, wird er auch immer mit genau diesen ausgeführt, unabhängig davon, welcher Anwender den Task dann tatsächlich startet.

- **Zeit-/ereignisgesteuerter oder verschobener Start**

  Anmeldedaten für den Task sind zwingend. Sie können die Task-Erstellung nicht abschließen, bevor Sie die Anmeldedaten für den Task spezifiziert haben. Anmeldedaten für den Task werden auf der Seite zur Task-Erstellung in ähnlicher Weise wie die Anmeldedaten für den Plan spezifiziert.

In Linux:

Sie müsse keine Anmeldedaten für Tasks spezifizieren. Unter Linux laufen Tasks immer unter dem Benutzerkonto 'root'.

3.3 Benutzerberechtigungen auf einer verwalteten Maschine

Windows

Der Umfang an Rechten, den ein Benutzer bei Verwaltung einer unter Windows laufenden Maschine hat, hängt von seinen allgemeinen Benutzerberechtigungen auf der jeweiligen Maschine ab.

Normale Benutzer

Ein normaler Benutzer, wie es etwa ein Mitglied der Gruppe 'Benutzer' ist, verfügt über folgende Verwaltungsrechte:

- Durchführung von Backup und Wiederherstellung auf Datei-Ebene, mit Dateien, auf die der Benutzer Zugriffsrechte hat – jedoch ohne Nutzung von Backup-Snapshots auf Datei-Ebene (S. 127).
- Backup-Pläne und Tasks erstellen und diese verwalten
- Die Backup-Pläne und Tasks anderer Nutzer können eingesehen, jedoch nicht verwaltet werden.
- Einsicht in die lokale Ereignisanzeige

Sicherungs-Operatoren

Ein Benutzer, der Mitglied der Gruppe 'Sicherungs-Operatoren' ist, hat folgendes Verwaltungsrecht:

- Backup und Wiederherstellung der kompletten Maschine oder von beliebigen Daten auf der Maschine, mit oder ohne Laufwerk-Snapshot Die Verwendung eines Hardware Snapshot Providers kann immer noch administrative Berechtigungen erfordern.

Administratoren

Ein Benutzer, der Mitglied der Gruppe 'Administratoren' ist, hat folgendes Verwaltungsrecht:

- Backup-Pläne und Tasks, die anderen Benutzern auf der Maschine gehören, einsehen und verwalten.

Linux

Bei Verwaltung einer unter Linux laufenden Maschine hat oder erhält der Benutzer root-Berechtigungen und kann daher:

- beliebige Daten oder die komplette Maschine sichern und wiederherstellen, mit voller Kontrolle über alle Aktionen des Acronis Backup & Recovery 11.5-Agenten und der Log-Dateien auf der Maschine.
- lokale Backup-Pläne und Tasks verwalten, die jedem beliebigen im Betriebssystem registrierten Anwender gehören.

Zur Vermeidung eines routinemäßigen Einloggens in das System als 'root' kann sich der Benutzer 'root' mit seinen gewöhnlichen Benutzer-Anmeldedaten einloggen und dann den Benutzer bei Bedarf wechseln.

3.4 Liste der Acronis Services (Dienste)

Acronis Backup & Recovery 11.5 erstellt während der Installation mehrere Dienste.

- Hauptdienste präsentieren die Hauptkomponenten von Acronis Backup & Recovery 11.5: der Agent, der Management Server, der Storage Node.
- Hilfsdienste ermöglichen bestimmte Funktionen der Hauptkomponenten.
- Allgemeine Dienste unterstützten mehrere Komponenten von Acronis Backup & Recovery 11.5 und andere Acronis-Produkte.

Die Dienste von Acronis Backup & Recovery 11.5-Komponenten

Ein Hauptdienst kann unter einem dedizierten Konto laufen oder einem von Ihnen spezifizierten Konto (während der Installation). Beiden Konton werden Berechtigungen gegeben, die erforderlich sind, damit der Dienst arbeiten kann. Diese Berechtigungen beinhalten eine Zusammenstellung von Benutzerrechten, Mitgliedschaft in Sicherheitsgruppen und die Erlaubnis zum **Vollzugriff** auf bestimmte Registry-Einträge in folgendem Schlüssel: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis. Es werden keine weiteren Berechtigungen für andere Registry-Schlüssel gewährt.

Die folgende Tabelle listet die Dienste von Acronis Backup & Recovery 11.5-Komponenten und die Berechtigungen für ihre Konten auf.

Name des Dienstes	Zweck	Vom Dienst verwendetes Konto	Dem Konto hinzugefügte Berechtigungen		
			Benutzerrechte	**Gruppenmitgliedschaft**	**Berechtigungen für Registry-Schlüssel**
Die Dienste von Acronis Backup & Recovery 11.5-Agenten					
Acronis Managed Machine Service (Hauptdienst)	Backup und Recovery von Daten auf der Maschine	**Acronis Agent User** *(neues Konto)* oder benutzerspezifiziertes Konto	**Als Dienst anmelden** **Anpassen von Speicherkontingenten für einen Prozess** **Ersetzen eines Token auf Prozessebene** **Verändern der Firmwareumgebungsvariablen**	**Sicherungs** **-Operatoren** *(für jedes Konto)* **Administratoren** *(nur für ein neues Konto)*	BackupAndRecovery Verschlüsselung Global MMS
Acronis VSS Provider (Hilfsdienst; nur für den Agenten für Windows in einem Windows Server -Betriebssystem erstellt)	Verwendung eines Volume Shadow Copy (VSS) Providers (S.142) (Volumenschattenkopie-Anbieter), der mit Acronis Backup & Recovery 11.5 ausgeliefert wird.	**Lokales System**	Keine zusätzlichen Berechtigungen		
Acronis Removable Storage Management Service (Hilfsdienst)	Verwaltung lokal angeschlossener Bandgeräte. Kann außerdem durch den Storage Node Service verwendet werden.	**Lokales System**	Keine zusätzlichen Berechtigungen		
Dienste für den Acronis Backup & Recovery 11.5 Management Server					
Acronis Management Server Service (Hauptdienst)	Zentrale Verwaltung von Backup-Aktionen auf mehreren Maschinen	**AMS User** *(neues Konto)* oder benutzerspezifiziertes Konto	**Als** **Dienst anmelden**	**Acronis Centralized Admins**	AMS BackupAndRecovery
SQL Server (ACRONIS) (Hilfsdienst; nur erstellt, falls ein neuer SQL-Server installiert wird)	Ausführung eines Microsoft SQL Server, der optional mit dem Management Server installiert wird	**Lokales System**	Keine zusätzlichen Berechtigungen		

Name des Dienstes	Zweck	Vom Dienst verwendetes Konto	Dem Konto hinzugefügte Berechtigungen		
			Benutzerrechte	Gruppenmit-gliedschaft	Berechtigungen für Registry-Schlüssel
Acronis Web Server Service (Hilfsdienst)	Hosting der Management Server-Webseite	Gleich wie beim Acronis Management Server Service			
Dienste für den Acronis Backup & Recovery 11.5 Storage Node					
Acronis Storage Node Service (Hauptdienst)	Verwaltung und Deduplizierung von Backup-Archiven, Aufrechterhaltung des zentralen Datenkatalogs.	**ASN User** *(neues Konto)* oder benutzerspezifi-ziertes Konto	**Als Dienst anmelden**	**Sicherungs-Operatoren** *(für jedes Konto)* **Administratoren** *(nur für ein neues Konto)*	ASN BackupAndRecovery Verschlüsselung
Acronis Removable Storage Management Service (Hilfsdienst)	Verwaltung lokal angeschlossener Bandgeräte. Kann außerdem durch den Managed Machine Service verwendet werden.	**Lokales System**	Keine zusätzlichen Berechtigungen		

Allgemeine Dienste (Common Services)

Folgende Dienste können von mehreren Komponenten von Acronis Backup & Recovery 11.5 sowie von anderen Acronis-Produkten verwendet werden. Diese Dienste laufen immer unter einem Systemkonto. Dem Konto werden keine zusätzlichen Berechtigungen gegeben.

Name des Dienstes	Zweck	Vom Dienst verwendetes Konto
Dienste für den Acronis PXE Server		
Acronis PXE Server Service	Machinen mit bootfähigen Komponenten (Acronis Bootable Components) über das Netzwerk booten	**Lokales System**
Acronis File Server Service	Bootfähige Komponenten für den Acronis PXE Server bereitstellen	**Lokales System**
Remote-Zugriff und Planungsdienste (Scheduling Services)		
Acronis Remote Agent Service	Stellt die Verbindungsmöglichkeit zwischen Acronis-Komponenten bereit.	**Lokales System** (Windows Vista und später) oder **NetworkService** (früher als Windows Vista)
Acronis Scheduler2 Service	Ermöglicht die Planung von durch Acronis-Komponenten durchgeführte Tasks.	**Lokales System**

Abhängigkeiten von anderen Diensten

Die Hauptdienste hängen vom Acronis Scheduler2 Service sowie folgenden Windows-Standarddiensten ab: **Remoteprozeduraufruf (RPC)** und **Geschützter Speicher**. Der Acronis Managed Machine Service und der Acronis Storage Node Service hängen außerdem vom Standarddienst **Windows-Verwaltungsinstrumentation** ab.

Gehen Sie folgendermaßen vor, um eine Liste der Abhängigkeiten für einen Dienst einzusehen:

1. Klicken Sie im Snap-in **Dienste** doppelt auf den Namen des Dienstes.
2. Betrachten Sie in der Registerkarte **Abhängigkeiten** das Feld **Dieser Dienst ist von diesen Systemkomponenten abhängig…**.

3.5 Vollständige, inkrementelle und differentielle Backups

Acronis Backup & Recovery 11.5 ermöglicht Ihnen, gängige Backup-Schemata (z.B. Großvater-Vater-Sohn oder „Türme von Hanoi") wie auch selbst erstellte Schemata zu verwenden. Alle Backup-Schemata basieren auf vollständigen, inkrementellen und differentiellen Backup-Methoden. Genau genommen kennzeichnet der Begriff „Schemata" den Algorithmus zur Anwendung dieser Methoden plus dem Algorithmus zur Backup-Bereinigung.

Backup-Methoden miteinander zu vergleichen macht nicht viel Sinn, da die Methoden als Team in einem Backup-Schema arbeiten. Jede Methode sollte abhängig von ihren Vorteilen ihre spezifische Rolle spielen. Ein sachgerechtes Backup-Schema profitiert von den Vorteilen und vermindert die Unzulänglichkeiten aller Backup-Methoden. So erleichtert z.B. ein wöchentliches differentielles Backup eine Archiv-Bereinigung, da es zusammen mit einem wöchentlichen Set täglicher, von ihm abhängender inkrementeller Backups mühelos gelöscht werden kann.

Mit vollständigen, inkrementellen oder differentiellen Backup-Methoden durchgeführte Sicherungen resultieren in Backups (S. 485) des jeweils entsprechenden Typs.

Voll-Backup

Ein vollständiges Backup speichert alle für ein Backup ausgewählten Daten. Ein Voll-Backup liegt jedem Archiv zugrunde und bildet die Basis für inkrementelle und differentielle Backups. Ein Archiv kann mehrere Voll-Backups enthalten oder nur aus Voll-Backups bestehen. Ein Voll-Backup ist autark – Sie benötigen also keinen Zugriff auf irgendein anderes Backup, um Daten aus diesem Voll-Backup wiederherzustellen.

Es ist weitgehend akzeptiert, dass ein Voll-Backup bei der Erstellung am langsamsten, aber bei der Wiederherstellung am schnellsten ist. Eine Wiederherstellung aus einem inkrementellen Backup ist dank Acronis-Technologien jedoch nicht langsamer als aus einem vollständigen Backup.

Ein Voll-Backup ist am nützlichsten, wenn:

- Sie ein System auf seinen Ausgangszustand zurückbringen wollen
- dieser Ausgangszustand sich nicht häufig ändert, so dass es keine Notwendigkeit für reguläre Backups gibt.

Beispiel: Ein Internet-Cafe, eine Schule oder ein Universitätslabor, wo der Administrator durch Studenten oder Gäste bewirkte Änderungen rückgängig macht, aber nur selten das Referenz-Backup aktualisiert (tatsächlich nur nach Installation neuer Software). In diesem Fall ist der Backup-Zeitpunkt nicht entscheidend, während die zur Wiederherstellung aus dem Voll-Backup benötigte Zeit minimal

ist. Zur Erreichung einer zusätzlichen Ausfallsicherheit kann der Administrator mehrere Kopien des Voll-Backups haben.

Inkrementelles Backup

Ein inkrementelles Backup speichert die Veränderungen der Daten in Bezug auf das **letzte Backup**. Sie benötigen Zugriff auf die anderen Backups des gleichen Archivs, um Daten aus einem inkrementellen Backup wiederherzustellen.

Ein inkrementelles Backup ist am nützlichsten, wenn:

- es möglich sein muss, die Daten zu jedem der multiplen, gespeicherten Zustände zurückzusetzen.
- die Veränderung der Daten im Vergleich zur Gesamtdatenmenge klein ist.

Es ist weitgehend akzeptiert, dass inkrementelle Backups weniger zuverlässig als Voll-Backups sind, da bei Beschädigung eines Backups innerhalb der „Kette“ auch die nachfolgenden nicht mehr verwendet werden können. Dennoch ist das Speichern mehrerer Voll-Backups keine Option, wenn Sie multiple frühere Versionen Ihrer Daten benötigen, da die Verlässlichkeit eines übergroßen Archivs noch fragwürdiger ist.

Beispiel: Das Backup eines Datenbank-Transaktions-Logs.

Differentielles Backup

Ein differentielles Backup speichert Änderungen an den Daten im Vergleich zum **letzten Voll-Backup**. Sie benötigen den Zugriff auf das entsprechende Voll-Backup, um die Daten aus einem differentiellen Backup wiederherzustellen. Ein differentielles Backup ist am nützlichsten, wenn:

- Sie daran interessiert sind, nur den neusten Datenzustand zu speichern.
- die Veränderung der Daten im Vergleich zur Gesamtdatenmenge klein ist.

Die typische Schlussfolgerung ist: Differentielle Backups sind langsamer bei Erstellung, aber schneller bei Wiederherstellung, während inkrementelle schneller zu erstellen, aber langsamer wiederherzustellen sind. Tatsächlich gibt es keinen physikalischen Unterschied zwischen einem an ein Voll-Backup angefügten, inkrementellen Backup und einem differentiellen Backup, welches demselben Voll-Backup zum gleichen Zeitpunkt angehängt wird. Der weiter oben erwähnte Unterschied setzt die Erstellung eines differentiellen Backups nach (oder statt) Erstellung multipler differentieller Backups voraus.

Ein nach Defragmentierung einer Festplatte erstelltes inkrementelles oder differentielles Backup kann beträchtlich größer als üblich sein, weil die Defragmentierung die Speicherposition von Dateien auf der Platte verändert und die Backups genau diese Veränderungen reflektieren. Es wird daher empfohlen, dass Sie nach einer Festplatten-Defragmentierung erneut ein Voll-Backup erstellen.

Die nachfolgende Tabelle fasst die allgemein bekannten Vorteile und Schwächen jedes Backup-Typs zusammen. Unter realen Bedingungen hängen diese Parameter von zahlreichen Faktoren ab, wie Menge, Größe und Muster der Datenveränderungen, Art der Daten, den physikalischen Spezifikationen der Geräte, den von Ihnen eingestellten Backup- bzw. Recovery-Optionen und einigen mehr. Praxis ist der beste Leitfaden für die Wahl des optimalen Backup-Schemas.

Parameter	Voll-Backup	Differentielles Backup	Inkrementelles Backup
Speicherplatz	Maximal	Medium	Minimal
Erstellungszeit	Maximal	Medium	Minimal
Wiederherstellungszeit	Minimal	Medium	Maximal

3.6 Was speichert das Backup eines Laufwerks oder Volumes?

Ein Laufwerk- bzw. Volume-Backup speichert das **Dateisystem** des entsprechenden Laufwerks bzw. Volumes 'als Ganzes'. Dabei werden auch alle zum Booten des Betriebssystems erforderlichen Informationen eingeschlossen. Aus solchen Backups können Laufwerke oder Volumes komplett wiederhergestellt werden – aber auch einzelne Dateien oder Ordner.

Windows

Ein Volume-Backup speichert alle Dateien und Ordner des gewählten Volumes, unabhängig von ihren Attributen (inkl. versteckter oder System-Dateien), den Boot-Record, die FAT (File Allocation Table) und – sofern vorhanden – auch das Stammverzeichnis (Root) und die Spur Null (Track Zero), inkl. Master Boot Record (MBR).

Ein Laufwerk-Backup speichert alle Volumes des betreffenden Laufwerks (inkl. versteckter Volumes wie Wartungs-Volumes von Herstellern) und die Spur Null (Track Zero) mit dem Master Boot Record (MBR).

Folgende Elemente sind in einem Laufwerk- oder Volume-Backup nicht enthalten (und genauso wenig in einem Backup auf Dateiebene):

- Die Auslagerungsdatei (pagefile.sys) und die Datei, die ein Abbild des Hauptspeichers ist, wenn der Computer in den Ruhezustand wechselt (hiberfil.sys). Nach einer Wiederherstellung werden die Dateien an passender Position mit einer Größe von Null erneut erzeugt.
- Windows Schattenspeicher (Shadow Storage). Der auf diesen verweisende Pfad wird über den Registry-Wert **VSS Default Provider** bestimmt, der im Registry-Schlüssel **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup** gefunden werden kann. Das bedeutet, dass bei Betriebssystemen beginnend mit Windows Vista keine Systemwiederherstellungspunkte von Windows per Backup gesichert werden.

Linux

Ein Volume-Backup speichert alle Dateien und Verzeichnisse des gewählten Laufwerkes (unabhängig von ihren Attributen), einen Boot-Record und den Dateisystem-Super-Block.

Ein Laufwerk-Backup speichert alle Volumes des Laufwerks, inkl. der Spur Null (Track Zero) mit dem 'Master Boot Record' (MBR).

Bei aktivierter **'Sektor-für-Sektor'-Option (Raw-Modus)** werden alle Sektoren des Laufwerks im Laufwerk-Backup gespeichert. Das Sektor-für-Sektor-Backup kann verwendet werden, um Laufwerke mit nicht erkannten oder nicht unterstützten Dateisystemen sowie anderen proprietären Datenformaten zu sichern.

3.7 Über dynamische und logische Volumes

3.7.1 Backup und Recovery von dynamischen Volumes (Windows)

Dieser Abschnitt erläutert in Kürze Backup und Wiederherstellung dynamischer Volumes (S. 491) durch Acronis Backup & Recovery 11.5.

Ein dynamisches Volume ist ein Volume, das sich auf einem dynamischen Laufwerk (S. 490) oder genauer auf einer Laufwerksgruppe (S. 488) befindet. Acronis Backup & Recovery 11.5 unterstützt die folgenden dynamischen Laufwerkstypen/RAID-Level:

- Einfach/Übergreifend
- Stripeset (RAID 0)
- Gespiegelt (RAID 1)
- eine Stripeset-Spiegelung (RAID 0+1)
- RAID -5.

Dynamische Volumes werden gesichert

Dynamische Volumes werden auf gleiche Weise wie Volumes vom Typ 'Basis' gesichert. Beim Erstellen eines Backup-Plans über die Benutzeroberfläche stehen all diese Laufwerkstypen als **Backup-Objekte** zur Auswahl. Wenn Sie die Befehlszeileneingabe verwenden, so spezifizieren Sie dynamische Volumes mit dem Präfix 'DYN'.

Befehlszeilen-Beispiele

```
acrocmd backup disk --volume=DYN1,DYN2 --loc=\\srv1\backups
--credentials=netuser1,pass1 --arc=dyn1_2_arc
```

Dies erstellt ein Backup der Volumes DYN1 und DYN2 in einen freigegebenen Netzwerkordner.

```
acrocmd backup disk --volume=DYN --loc=\\srv1\backups --credentials=netuser1,pass1
--arc=alldyn_arc
```

Dies erstellt ein Backup aller dynamischen Volumes der lokalen Maschine zu einem freigegebenen Netzwerkordner.

Dynamische Volumes werden wiederhergestellt

Ein dynamisches Volume kann wiederhergestellt werden:

- Über jeden existierenden Volume-Typ.
- Auf dem 'nicht zugeordneten' Speicherplatz einer Laufwerksgruppe.
- Auf dem 'nicht zugeordneten' Speicherplatz eines Basis-Laufwerks.
- Auf einem noch nicht initialisierten Laufwerk.

Recovery über ein existierendes Laufwerk

Wenn ein dynamisches Laufwerk über ein existierendes Laufwerk ('Basis' oder 'dynamisch) wiederhergestellt wird, so werden die Daten des Ziellaufwerks mit dem Inhalt des Backups überschrieben. Der Typ des Ziellaufwerkes (Basis, einfach/übergreifend, Stripeset, gespiegelt, RAID 0+1, RAID -5) wird nicht verändert. Die Größe des Ziellaufwerkes muss ausreichend sein, um den Inhalt des Backups aufnehmen zu können.

Recovery zu nicht zugeordneten Speicherplatz einer Laufwerksgruppe

Wenn Sie ein dynamisches Volume zu dem 'nicht zugeordneten' Speicherplatz einer Laufwerksgruppe wiederherstellen, bewahrt die Software den Typ und die Größe des ursprünglichen Volumes. Sollte die Laufwerksgruppenkonfiguration den ursprünglichen Volume-Typ nicht erlauben, dann wird das Volume mit dem Typ 'Einfach' (Simple) oder 'Übergreifend' (Spanned) wiederhergestellt. Falls das Volume auf den 'nicht zugeordneten' Speicherplatz nicht passen sollte, dann erfolgt eine Größenanpassung des Volumes durch Verkleinerung seines freien Speicherplatzes.

Beispiele für Szenarien, in denen die Laufwerksgruppenkonfiguration den ursprünglichen Typ des Volumes nicht erlaubt

Beispiel 1. Die Gruppe enthält weniger Laufwerke als für das dynamische Volume erforderlich sind. Angenommen, Sie sind dabei, ein auf 3 Laufwerken liegendes RAID-5-Volume mit 80 GB auf eine Laufwerksgruppe wiederherzustellen, die aus zwei Laufwerken besteht. Die Gesamtgröße

des 'nicht zugeordneten' Speicherplatzes beträgt 100 GB: 40 GB auf dem ersten Laufwerk und 60 GB auf dem zweiten. Das RAID-5-Volume wird als übergreifendes Volume (Spanned) über zwei Laufwerke wiederhergestellt.

Beispiel 2. Die Verteilung des 'nicht zugeordneten' Speicherplatzes erlaubt keine Wiederherstellung von dynamischen Volumes eines bestimmten Typs. Angenommen, Sie wollen ein 30 GB-Stripeset-Volume auf eine Laufwerksgruppe wiederherstellen, die aus zwei Laufwerken besteht. Die Gesamtgröße des 'nicht zugeordneten' Speicherplatzes beträgt 50 GB: 10 GB auf dem ersten Laufwerk und 40 GB auf dem zweiten. Das Stripeset-Volume wird mit dem Typ 'Einfach' (Simple) auf dem zweiten Laufwerk wiederhergestellt.

Recovery auf ein noch nicht initialisiertes Laufwerk

In diesem Fall wird das Ziellaufwerk automatisch mit dem Partitionsschema MBR initialisiert. Die dynamischen Volumes werden als Volumes vom Typ 'Basis' wiederherstellt. Falls die Volumes auf den 'nicht zugeordneten' Speicherplatz nicht passen sollten, wird ihre Größe proportional angepasst (durch Verringerung ihres freien Speicherplatzes).

Die untere Tabelle demonstriert die resultierenden Volume-Typen, abhängig von Backup-Quelle und Recovery-Ziel.

	Backup (Quelle):	
Wiederhergestellt zu:	**Dynamisches Volume**	**Basis-Volume**
Dynamisches Volume	Dynamisches Volume Typ wie der des Ziels	Dynamisches Volume Typ wie der des Ziels
Nicht zugeordneter Speicherplatz (Laufwerksgruppe)	Dynamisches Volume Typ wie der des Ziels	Dynamisches Volume Einfach
Basis-Volume oder 'nicht zugeordneter' Speicherplatz auf einem Basis-Laufwerk	Basis-Volume	Basis-Volume

Laufwerke während einer Wiederherstellung verschieben und in der Größe anpassen

Sie können das resultierende Basis-Volume während der Wiederherstellung manuell in der Größe anpassen oder seine Position auf dem Laufwerk ändern. Ein resultierendes dynamisches Volume kann nicht manuell verschoben oder in seiner Größe angepasst werden.

Datenträgergruppen und Laufwerke vorbereiten

Vor Wiederherstellung eines dynamischen Volumes auf ein fabrikneues System sollten Sie auf der Ziel-Hardware eine Laufwerksgruppe erstellen.

Möglicherweise müssen Sie auch verfügbaren, nicht zugeordneten Speicherplatz auf einer existierenden Laufwerksgruppe erstellen oder vergrößern. Dies kann durch Löschen von Laufwerken oder Konvertieren von Basis- zu dynamischen Datenträgern umgesetzt werden.

Möglicherweise wollen Sie den Typ des Ziel-Volumes ändern (Basis, einfach/übergreifend, Stripeset, gespiegelt, RAID 0+1, RAID 5). Dies kann durch Löschen des Ziellaufwerks und Erstellung eines neuen Laufwerks auf dem resultierenden 'nicht zugeordneten' Speicherplatz durchgeführt werden.

Acronis Backup & Recovery 11.5 enthält ein nützliches Disk Management Utility, welches Ihnen die Durchführung der oberen Aktionen ermöglicht (unter einem Betriebssystem oder direkt auf einem fabrikneuen System). Zu weiteren Informationen über Acronis Disk Director Lite siehe den Abschnitt Laufwerksverwaltung (S. 300).

3.7.2 Backup und Recovery von logischen Volumes und MD-Geräten (Linux)

Dieser Abschnitt erläutert, wie Sie Volumes, die durch den 'Logical Volume Manager' (LVM) von Linux verwaltet werden (logische Volumes genannt), sowie Multiple-Disk- bzw. MD-Geräte (Linux Software-RAID genannt) per Backup sichern und wiederherstellen können.

Um mehr über LVM zu erfahren, besuchen Sie die (englischsprachigen) Webseiten http://tldp.org/HOWTO/LVM-HOWTO/ oder http://www.centos.org/docs/5/html/5.1/Deployment_Guide/ch-lvm.html.

3.7.2.1 Backup von logischen Volumes

Der Acronis Backup & Recovery 11.5 Agent für Linux kann auf logische Volumes zugreifen, sie sichern und wiederherstellen, wenn er unter Linux (ab Kernel 2.6) oder einem Linux-basierten Boot-Medium ausgeführt wird.

Backup

Logische Volumes erscheinen in der Benutzeroberfläche von Acronis Backup & Recovery 11.5 unter **Dynamische Volumes** am Ende der Liste aller zum Backup verfügbarer Volumes. Wenn Sie ein logisches Volume zum Backup auswählen, dann wird zusammen mit seinem Inhalt auch die Volume-Struktur gesichert. Diese Struktur kann automatisch neu erstellt werden, wenn Sie ein solches Volume unter einem Linux-basierten bootfähigen Medium wiederherstellen.

Um alle verfügbaren Laufwerke zu sichern, spezifizieren Sie alle logischen Volumes sowie alle unabhängigen Basis-Volumes (die nicht zu den logischen Volumes gehören). Das ist die vorgegebene Auswahl, wenn Sie die Seite **Backup-Plan erstellen** öffnen.

In logischen Volumes enthaltene Basis-Volumes werden innerhalb der Liste mit der Kennzeichnung **Kein** in der Spalte **Dateisystem** angezeigt. Wenn Sie solche Volumes auswählen, sichert das Programm diese per Sektor-für-Sektor-Backup. Normalerweise ist dies nicht erforderlich.

Recovery

Bei der Wiederherstellung logischer Volumes haben Sie zwei Optionen:

- **Nur Volume-Inhalt wiederherstellen**. Der Typ oder andere Eigenschaften des Ziel-Volumes werden nicht geändert.

  Diese Option ist sowohl im Betriebssystem wie auch unter einem bootfähigen Medium verfügbar.

  Diese Option ist in folgenden Fällen nützlich:

  - Wenn auf dem Volume einige Daten verloren gegangen sind, aber keine Laufwerke ersetzt wurden.
  - Wenn Sie ein logisches Volume über ein Laufwerk bzw. Volume vom Typ 'Basis' wiederherstellen. Sie können in diesem Fall die Größe des resultierenden Volumes anpassen.

    Ein System, bei dem das Backup eines logischen Volumes auf einem Basis-Laufwerk wiederhergestellt wurde, ist nicht bootfähig, da sein Kernel versucht, das Root-Dateisystem beim logischen Volume zu mounten. Um das System zu booten, ändern Sie die Loader-Konfiguration und '/etc/fstab' (so dass LVM nicht verwendet wird) und reaktivieren Sie Ihren Boot-Loader (S. 177).

  - Wenn Sie eine Basis-Volume oder logisches Volume zu einem bereits existierenden Volume wiederherstellen.

Falls sich das Boot-Volume (/boot) auf einem Basis-Volume befand, empfehlen wir, es auch auf einem Basis-Volume wiederherzustellen – und das sogar dann, wenn Ihr Boot-Loader das Booten von logischen Volumes unterstützt.

- **Die Struktur logischer Volumes und gleichzeitig ihre Inhalte wiederherstellen**.

  Das ist der Fall, wenn Sie auf fabrikneue Geräte wiederherstellen oder auf eine Maschine mit anderer Volume-Struktur. Die Struktur logischer Volumes kann automatisch zum Zeitpunkt einer Recovery-Aktion erstellt werden (S. 49).

  Diese Option ist nur verfügbar, wenn Sie unter einem Boot-Medium arbeiten.

Zu weiteren Informationen über die Wiederherstellung logischer Volumes siehe Wiederherstellung von MD-Gerдten und logischen Volumes (S. 48).

3.7.2.2 Backup von MD-Geräten

MD-Geräte (auch bekannt als Linux-Software-RAID) kombinieren mehrere Volumes und erstellen 'Solid Block Devices' (**/dev/md0, /dev/md1, ..., /dev/md31**). Die Informationen über MD-Geräte werden in **/etc/raidtab** oder in speziellen Bereichen dieser Volumes gespeichert.

Sie können aktive (gemountete) MD-Geräte auf dieselbe Art wie logische Volumes per Backup sichern. Die MD-Geräte erscheinen am Ende der für Backups verfügbaren Volume-Liste. Wenn Sie ein MD-Gerät zum Backup auswählen, dann wird zusammen mit seinem Inhalt auch die Struktur des MD-Gerätes gesichert.

Wenn ein MD-Gerät gemountet ist, macht es keinen Sinn, die im MD-Gerät enthaltenen Volumes per Backup zu sichern, weil es nämlich nicht möglich ist, diese auch wiederherzustellen.

Wenn Sie ein MD-Gerät unter einem bootfähigen Medium wiederherstellen, kann die Struktur des MD-Gerätes automatisch neu erstellt werden. Zu weiteren Informationen über die Wiederherstellung von MD-Geräten unter bootfähigen Medien siehe MD-Gerдte und logische Volumes wiederherstellen (S. 48).

Zu weiteren Informationen über die Erstellung von MD-Geräten bei Recovery-Aktionen unter Linux siehe MD-Gerдte fьr eine Wiederherstellung zusammenstellen (Linux) (S. 47).

3.7.2.3 Backup von Hardware-RAID-Arrays (Linux)

Hardware-RAID-Arrays unter Linux kombinieren mehrere physikalische Laufwerke, um ein als Einheit partitionierbares Laufwerk zu erstellen. Die spezielle, auf ein Hardware-RAID-Array bezogene Datei befindet sich üblicherweise unter /dev/ataraid. Sie können Hardware-RAID-Arrays auf dieselbe Art wie gewöhnliche Festplatten per Backup sichern.

Physikalische Laufwerke, die Teil eines Hardware-RAID-Arrays sind, können neben anderen Laufwerken so aufgelistet sein, als ob sie eine beschädigte oder überhaupt keine Partitionstabelle haben würden. Solche Laufwerke per Backup zu sichern macht keinen Sinn, wie es auch nicht möglich ist, sie wiederherzustellen.

3.7.2.4 MD-Geräte für eine Wiederherstellung zusammenstellen (Linux)

Wenn Sie in Linux eine Wiederherstellung von einem Laufwerk-Backup auf ein existierendes MD-Gerät (auch Linux Software-RAID genannt) durchführen, dann stellen Sie sicher, dass dieses **Gerät zusammengestellt** ist (zum Zeitpunkt der Wiederherstellung).

Ist das Gerät nicht verfügbar, so holen Sie dies durch Verwendung des Utilities **mdadm** nach. Hier sind zwei Beispiele:

Beispiel 1. Der folgende Befehl erstellt das Gerät /dev/md0, kombiniert aus den Volumes /dev/sdb1 und /dev/sdc1:

```
mdadm --assemble /dev/md0 -ayes /dev/sdb1 /sdc1
```

Beispiel 2. Der folgende Befehl erstellt das Gerät /dev/md0, kombiniert aus den Disks /dev/sdb und /dev/sdc:

```
mdadm --assemble /dev/md0 -ayes /dev/sdb /dev/sdc
```

Orientieren Sie sich an den nachfolgenden Anleitungen, wenn für die Wiederherstellung ein Neustart der Maschine erforderlich ist (üblich, falls die wiederherzustellenden Volumes ein Boot-Volume enthält):

- Wenn alle Teile des MD-Gerätes Volumes sind (typischer Fall, so wie im ersten Beispiel), dann stellen Sie sicher, dass der Typ eines jeden Volumes (Partitionstyp oder System-ID genannt) vom Typ '**Linux raid automount**' ist — der Hexadezimal-Code dieses Volume- bzw. Partitionstypes ist 0xFD. Dies garantiert, dass das Gerät nach dem Neustart automatisch zusammengestellt wird. Verwenden Sie ein Partitionierungswerkzeug wie **fdisk**, um den Volume-Typ einzusehen oder zu verändern.
- Führen Sie anderenfalls (wie im zweiten Beispiel) die Recovery-Aktion von einem bootfähigen Medium aus. In diesem Fall ist auch kein Neustart erforderlich. Bei Verwendung bootfähiger Medien müssen Sie das MD-Gerät vermutlich manuell oder automatisch erstellen, wie unter MD-Gerдte und logische Volumes wiederherstellen (S. 48) beschrieben.

3.7.2.5 MD-Geräte und logische Volumes wiederherstellen

Bei der Wiederherstellung von MD-Geräten und/oder per Logical Volume Manager erstellten Volumes (logische Volumes) wird angenommen, dass die entsprechende Volume-Struktur neu erstellt wird.

Bei Linux-basierten bootfähigen Medien können Sie wählen, ob die Volume-Struktur automatisch wiederhergestellt werden soll (S. 49).

Diese Funktionalität ist insbesondere zur Wiederherstellungen einer kompletten Maschine auf fabrikneue Hardware (Bare Metal Recovery) gedacht. Die Software sichert die komplette logische Volume-Struktur und erstellt diese neu – und das sogar, wenn nicht alle MD-Geräte oder logischen Volumes gesichert oder wiederhergestellt wurden. Sie benötigen daher mindestens so viele Laufwerke, wie sie die ursprüngliche Volume-Struktur genutzt hat.

Versuchen Sie in folgenden Fällen nicht, die Volume-Struktur automatisch neu zu erstellen:

- Die Maschine hat **Daten, die bewahrt werden müssen**. Die Software wird alle Daten auf denjenigen Laufwerken zerstören, die sie zum Neuerstellen der Volume-Struktur auswählt.
- Die Maschine hat **weniger physikalische Laufwerke**, als sie von der ursprünglichen Volume-Struktur genutzt wurden. Die Software wird mit der Neuerstellung der Volume-Struktur fehlschlagen. Das gilt selbst dann, wenn die Kapazität der physikalischen Laufwerke ausreicht, um alle wiederhergestellten Daten aufzunehmen.
- Das Backup **enthält keine Volume-Strukturinformationen.** Diese Informationen können bei Backups fehlen, die mit Acronis Backup & Recovery 10 erstellt wurden, weil das Speichern der Informationen dort optional war.

In diesem Fall müssen Sie die Volume-Struktur manuell erstellen (S. 49) (vor der Wiederherstellung). Sie können dazu die Utilitys **mdadm** und **lvm** verwenden, entweder unter einem Linux-basierten Boot-Medium oder unter Linux selbst.

Volume-Struktur automatisch erstellen

Verwenden Sie die folgende Prozedur, um die logische Volume-Struktur auf einer Maschine automatisch neu zu erstellen.

Achtung! *– Als Ergebnis der nachfolgenden Prozedur wird die aktuelle Volume-Struktur auf der Maschine durch die im Backup gespeicherte Struktur ersetzt. Damit werden die aktuell auf einigen bzw. allen Laufwerken der Maschine gespeicherten Daten gelöscht.*

Falls sich die Laufwerkskonfiguration geändert hat. Ein MD-Gerät oder ein logisches Volume befindet sich auf einem oder mehreren Laufwerk(en). Wenn Sie eines dieser Laufwerke zwischen Backup und Wiederherstellung ausgetauscht haben (oder falls Sie die Volumes zu einer anderen Maschine wiederherstellen), dann müssen Sie sicherstellen, dass die neue Laufwerkskonfiguration mindestens dieselbe Anzahl an Laufwerken beinhaltet wie die ursprüngliche Volume-Struktur. Die Kapazität der Laufwerke muss ausreichend sein, um alle wiederherzustellenden Daten aufnehmen zu können.

So erstellen Sie die Volume-Struktur automatisch

1. Booten Sie die Maschine mit einem Linux-basierten bootfähigen Medium.
2. Klicken Sie auf **Acronis Bootable Agent**. Wählen Sie dann **Management Konsole starten**.
3. Klicken Sie in der Management Konsole auf den Befehl **Recovery**.

   Unter dem Inhalt des Archivs zeigt Acronis Backup & Recovery 11.5 eine Meldung an, dass Informationen über die Volume-Struktur gefunden wurden.
4. Klicken Sie in dem Bereich, in dem die Meldung erscheint, auf **Details**.
5. Überprüfen Sie die Volume-Struktur und klicken Sie dann auf **RAID/LVM anwenden** um sie zu erstellen.

Volume-Struktur manuell erstellen

Das Nachfolgende beschreibt eine allgemeine Prozedur und ein Beispiel für eine Wiederherstellung von MD-Geräten sowie logischen Volumes durch Verwendung eines Linux-basierten bootfähigen Mediums. Sie können ein ähnliches Verfahren unter Linux nutzen.

So erstellen Sie die Volume-Struktur manuell

1. Booten Sie die Maschine mit einem Linux-basierten bootfähigen Medium.
2. Klicken Sie auf **Acronis Backup & Recovery 11.5**. Wählen Sie dann **Management Konsole starten**.
3. Klicken Sie in der Symbolleiste auf **Aktionen** und dann **Shell starten**. Alternativ können Sie auch Strg+Alt+F2 drücken.
4. Falls erforderlich, können Sie die Struktur der im Archiv gespeicherten Volumes durch Verwendung des Werkzeugs **acrocmd** untersuchen. Sie können das Werkzeug außerdem auch dazu verwenden, eines oder mehrere dieser Volumes wie reguläre Volumes zu mounten (siehe #Backup-Volumes mounten# im weiteren Verlauf dieses Themas).
5. Erstellen Sie eine dem Archiv entsprechende Volume-Struktur durch Verwendung des Werkzeugs **mdadm** (für MD-Geräte), des Werkzeugs **lvm** (für logische Volumes) oder durch beide.

   Anmerkung: *'Logical Volume Manager'-Werkzeuge wie* ***pvcreate*** *und* ***vgcreate****, die üblicherweise unter Linux verfügbar sind, sind auf dem Boot-Medium nicht enthalten, so dass Sie das* ***lvm****-Werkzeug mit einem*

korrespondierenden Befehl verwenden müssen. Beispielsweise: ***lvm pvcreate****,* ***lvm vgcreate*** *und* ***lvm lvcreate****.*

6. Falls Sie das Backup bereits zuvor durch Verwendung des **acrocmd**-Werkzeugs gemountet haben, dann verwenden Sie das Utility erneut, um das Backup wieder zu trennen (siehe „Backup-Volumes mounten“ im weiteren Verlauf dieses Themas).
7. Wechseln Sie durch Drücken der Tastenkombination Alt+F1 zurück zur Management Konsole.

   (Starten Sie die Maschine an dieser Stelle nicht neu. Ansonsten müssen Sie die Volume-Struktur erneut erstellen.)
8. Klicken Sie auf **Recovery**, spezifizieren Sie dann den Pfad zum Archiv sowie andere benötigte Parameter und klicken Sie dann **OK**.

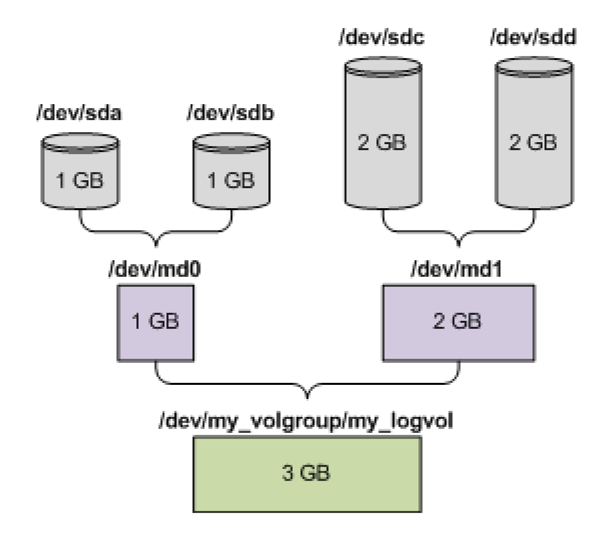
Anmerkung: *Diese Prozedur funktioniert nicht, wenn Sie sich remote zum Acronis Backup & Recovery 11.5 Bootable Agent verbinden, weil in diesem Fall die Eingabeaufforderung nicht verfügbar ist.*

Beispiel

Angenommen, Sie haben eine Maschine mit folgender Laufwerkskonfiguration über ein Laufwerk-basiertes Backup gesichert:

- Die Maschine hat zwei 1-Gigabyte und zwei 2-Gigabyte-SCSI-Laufwerke, die als **/dev/sda**, **/dev/sdb**, **/dev/sdc** beziehungsweise **/dev/sdd** angeschlossen sind.
- Die ersten und zweiten Laufwerkspaare sind als zwei MD-Geräte konfiguriert, beide in RAID-1-Konfiguration – und angeschlossen als **/dev/md0** bzw. **/dev/md1**.
- Ein logisches Volume basiert auf den beiden MD-Geräten und ist an **/dev/my_volgroup/my_logvol** gemountet.

Das folgende Bild illustriert diese Konfiguration.



Stellen Sie Daten von diesem Archiv wie folgt wieder her.

Schritt 1: Erstellung der Volume-Struktur

1. Booten Sie die Maschine mit einem Linux-basierten bootfähigen Medium.
2. Drücken Sie Strg+Alt+F2 in der Management Konsole.
3. Führen Sie folgenden Befehle aus, um die MD-Geräte zu erstellen:

```
mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sd[ab]
mdadm --create /dev/md1 --level=1 --raid-devices=2 /dev/sd[cd]
```

4. Führen Sie folgende Befehle aus, um die logische Volume-Gruppe zu erstellen:

Vorsicht: *Der Befehl* ***pvcreate*** *zerstört alle Daten auf den Geräten* ***/dev/md0*** *und* ***/dev/md1****.*

```
lvm pvcreate /dev/md0 /dev/md1
lvm vgcreate my_volgroup /dev/md0 /dev/md1
lvm vgdisplay
```

Die Ausgabe des **lvm vgdisplay**-Befehls wird Zeilen ähnlich wie diese enthalten:

```
--- Volume group ---
VG Name     my_volgroup
...
VG Access   read/write
VG Status   resizable
...
VG Size     1.99 GB
...
VG UUID     0qoQ4l-Vk7W-yDG3-uF1l-Q2AL-C0z0-vMeACu
```

5. Führen Sie folgenden Befehl aus, um das logische Volume zu erstellen; wobei Sie im **-L**-Parameter die gegebene Größe durch **VG Size** spezifizieren:

```
lvm lvcreate -L1.99G --name my_logvol my_volgroup
```

6. Aktivieren Sie die Volume-Gruppe durch Ausführung folgenden Befehls:

```
lvm vgchange -a y my_volgroup
```

7. Drücken Sie Alt+F1, um zur Management Konsole zurückzukehren.

Schritt 2: Start der Wiederherstellung

1. Wählen Sie in der Management Konsole den Befehl **Recovery**.
2. Wählen Sie bei **Archiv** den Befehl **Ändern** und spezifizieren Sie den Archivnamen.
3. Wählen Sie bei **Backup** den Befehl **Ändern** und dann das Backup, aus dem Sie die Daten wiederherstellen möchten.
4. Wählen Sie bei **Datentyp** den Befehl **Volumes**.
5. Aktivieren Sie bei **Wiederherzustellende Elemente** das Kontrollkästchen neben **my_volgroup-my_logvol**.
6. Wählen Sie unter **Recovery-Ziel** den Befehl **Ändern** und aktivieren Sie jenes logische Volume, das Sie in Schritt 1 erzeugt haben. Nutzen Sie die Chevron-Symbole zum Aufklappen der Laufwerksliste.
7. Wählen Sie **OK**, um die Wiederherstellung zu starten.

Für eine vollständige Liste aller Befehle und Utilities, die Sie in der Betriebssystemumgebung des Boot-Mediums verwenden können, siehe 'Liste verfьgbarer Befehle und Werkzeuge in Linux-basierten bootfдhigen Medien (S. 296)'. Eine detaillierte Beschreibung des **acrocmd**-Werkzeugs finden Sie in der Acronis Backup & Recovery 11.5-Befehlszeilen-Referenz.

Backup-Volumes mounten

Möglicherweise wollen Sie ein in einem Laufwerk-Backup gespeichertes Volume mounten, um einige Dateien vor Beginn einer Wiederherstellung einzusehen.

So mounten Sie ein Backup-Volume

1. Verwenden Sie den Befehl **acrocmd list content**, um die im Backup gespeicherten Laufwerke und Volumes aufzulisten. Folgender Befehl listet beispielsweise den Inhalt des jüngsten Backups eines Archivs mit der Bezeichnung **linux_machine** auf:

```
acrocmd list content --loc=\\server\backups --credentials=user,MyPassWd
--arc=linux_machine
```

Die Ausgabe wird Zeilen ähnlich wie diese enthalten:

```
type: disk
Num          Partition               Flags        Size         Type            GUID
----------   --------------------   ----------   ----------   -------------   ------
--
Dyn1         my_volgroup-my_lo...                 4 GB         Ext 3
Dyn2         md0                                  2.007 GB     Ext 2
Disk 1       sda                                  16 GB        DT_FIXED
1-1          sda1                    Act,Pri      203.9 MB     Ext 2
1-2          sda2                    Pri          11.72 GB     Reiser
1-3          sda3                    Pri          1.004 GB     Linux swap
Disk 2       sdb                                  8 GB         DT_FIXED
2-1          sdb1                    Pri          2.007 GB     Ext 2
2-2          sdb2                    Pri          2.007 GB     None
Disk 3       sdc                                  1 GB         DT_FIXED
Disk 4       sdd                                  8 GB         DT_FIXED
4-1          sdd1                    Pri          2.007 GB     Ext 2
4-2          sdd2                    Pri          2.007 GB     None
```

2. Verwenden Sie den Befehl **acrocmd mount**, wobei Sie den Volume-Namen über den Parameter **--volume** spezifizieren. Beispielsweise:

```
acrocmd mount --loc=\\server\backups --arc=linux_machine --mount_point=/mnt
--volume=DYN1
```

Dieser Befehl mountet das logische Volume DYN1 an den Mount-Punkt /mnt.

So trennen Sie ein Backup-Volume wieder (unmounting)

- Verwenden Sie den Befehl **acrocmd umount**, wobei Sie den Mount-Punkt des Volumes als Parameter spezifizieren. Beispielsweise:

```
acrocmd umount --mount_point=/mnt
```

3.8 Unterstützung für Festplatten mit Advanced Format (4K-Sektoren)

Acronis Backup & Recovery 11.5 kann sowohl Backups von Festplatten mit einer Sektorgröße von 4 KB erstellen (auch bekannt als Advanced Format-Laufwerke), wie auch von herkömmlichen Festplatten, die 512-Byte-Sektoren haben.

Acronis Backup & Recovery 11.5 kann Daten von einem dieser Laufwerke zu einem anderen wiederherstellen, solange *beide Laufwerke dieselbe logische Sektorgröße haben*. (Dies ist die gegenüber dem Betriebssystem präsentierte Sektorgröße.) Acronis Backup & Recovery 11.5 führt automatisch ein Alignment der Laufwerks-Volumes (S. 161) aus, sofern dies erforderlich ist. Auf diese Weise stimmt der Start eines Clusters im Dateisystem immer mit dem Start eines physikalischen Sektors auf dem Laufwerk überein.

Die Funktionalität zur Laufwerksverwaltungs (S. 300) von Acronis Backup & Recovery 11.5 steht für Laufwerke mit einer logischen Sektorgröße von 4-KB nicht zur Verfügung.

Bestimmung der logischen Sektorgröße

Anhand der Laufwerksspezifikation

Die Entwicklung der Advanced Format-Technologie wird von der 'International Disk Drive Equipment and Materials Association' (IDEMA) koordiniert. Weitere Details finden Sie unter http://www.idema.org/?page_id=2.

In Bezug auf die logische Sektorgröße spezifiziert die IDEMA zwei Typen von Advanced Format-Laufwerken:

- Laufwerke mit **512 Byte-Emulation (512e)** haben eine logische Sektorgröße von 512 Byte. Diese Laufwerke werden von Windows beginnend mit Windows Vista und von modernen Linux-Distributionen unterstützt. Microsoft und Western Digital verwenden den Ausdruck 'Advanced Format' exklusiv nur für diesen Laufwerkstyp.
- Laufwerke vom Typ **4K nativ (4Kn)** haben eine logische Sektorgröße von 4-KByte. Moderne Betriebssystem können Daten auf solchen Laufwerken speichern, meistens aber nicht von ihnen booten. Solche Laufwerken sind üblicherweise externe Laufwerke mit USB-Verbindung.

Durch Ausführung eines entsprechenden Befehls

Gehen Sie folgendermaßen vor, um die logische Sektorgröße eines Laufwerks zu ermitteln.

In Windows:

1. Stellen Sie sicher, dass das Laufwerk ein NTFS-Volume enthält.
2. Führen Sie folgenden Befehl als Administrator aus, unter Angabe des Laufwerksbuchstaben für das NTFS-Volume:
```
fsutil fsinfo ntfsinfo D:
```
3. Bestimmen Sie den Wert in der Zeile **Bytes pro Sektor**. Die Ausgabe kann beispielsweise wie folgt aussehen:
```
Bytes pro Sektor: 512
```

In Linux:

1. Ermitteln Sie den Gerätenamen des Laufwerks, wie etwa /dev/sdb.
2. Führen Sie folgenden Befehl als Benutzer 'root' aus, unter Angabe des Gerätenamens:
```
parted /dev/sdb print
```
3. Bestimmen Sie den ersten Wert in der Zeile **Sektorgröße (logisch/physisch)**. Die Ausgabe kann beispielsweise wie folgt aussehen:
```
Sektorgröße (logisch/physisch): 512B/4096B
```

3.9 Unterstützung für UEFI-basierte Maschinen

Acronis Backup & Recovery 11.5 kann Maschinen, die 64-Bit-UEFI (Unified Extensible Firmware Interface) verwenden, auf die gleiche Art sichern und wiederherstellen, wie es für Maschinen der Fall ist, die BIOS zum Booten verwenden.

Das gilt für physikalische und virtuelle Maschinen; und auch unabhängig davon, ob die virtuellen Maschinen auf Hypervisor-Ebene oder innerhalb eines Gast-Betriebssystems gesichert werden.

Backup und Recovery von Geräten, die 32-Bit-UEFI verwenden, wird nicht unterstützt.

Beschränkungen

- WinPE-basierte bootfähige Medien mit einer Version vor 4.0 und der Acronis PXE Server unterstützen kein Booten per UEFI.
- Acronis Active Restore (S. 484) steht auf UEFI-Maschinen nicht zur Verfügung.
- Acronis Startup Recovery Manager (ASRM) (S. 484) steht auf unter Linux laufenden UEFI-Maschinen nicht zur Verfügung. Aktivieren Sie auf unter Windows laufenden UEFI-Maschinen den ASRM von Windows aus, statt von einem bootfähigen Medium aus.

- Eine unter Linux laufende Maschine kann nicht zwischen UEFI und BIOS überführt werden. Weitere Details zum Überführen von Windows-Maschinen finden Sie im Abschnitt 'Recovery von BIOS-basierten Systemen zu UEFI-basierten Systemen und umgekehrt (S. 169)'.

3.10 Unterstützung für Windows 8 und Windows Server 2012

Dieser Abschnitt beschreibt, wie Acronis Backup & Recovery 11.5 Funktionen unterstützt, die mit den Windows 8- und Windows Server 2012-Betriebssystemen eingeführt wurden.

Die Informationen in diesem Abschnitt gelten außerdem für Windows 8.1 und den Windows Server 2012 R2.

Beschränkungen

- Der Acronis Disk Director Lite (S. 300) ist unter Windows 8 und dem Windows Server 2012 nicht verfügbar.
- Aktionen zur Laufwerksverwaltung funktionieren unter einem bootfähigen Medium möglicherweise nicht korrekt, falls auf der Maschine Speicherplätze (Storage Spaces) konfiguriert sind.
- Die Windows To Go-Funktion von Windows 8 wird nicht unterstützt.

WinPE 4.0 und WinPE 5.0

Der Acronis Media Builder kann bootfähige Medien erstellen, die auf diesen Versionen von Windows Preinstallation Environment (WinPE) basieren.

Diese bootfähigen Medien unterstützen neue Funktionen von Windows 8 und dem Windows Server 2012 (siehe weiter unten in diesem Abschnitt). Sie können auf bzw. mit Maschinen booten, die UEFI (Unified Extensible Firmware Interface) verwenden.

Sie benötigen zur Erstellung von bootfähigen Medien, die auf diesen WinPE-Versionen basieren, das Windows Assessment and Deployment Kit (ADK) Weitere Details finden Sie im Abschnitt 'WinPE-basierte bootfдhige Medien (S. 290)'.

UEFI Secure Boot

Auf einer unter Windows 8 oder Windows Server 2012 laufenden Maschine, die UEFI verwendet, kann die UEFI-Funktion 'Secure Boot' (auch 'Sicherer Start' genannt) angeschaltet sein. Secure Boot gewährleistet, dass die Maschine nur von vertrauenswürdigen Boot-Loadern gestartet werden kann.

Durch Verwendung des Acronis Media Builder können Sie ein bootfähiges Medium erstellen, das über einen vertrauenswürdigen Boot-Loader verfügt. Wählen Sie dazu, dass ein Linux-basiertes 64-Bit-Medium oder ein auf WinPE 4 (oder höher) basierendes 64-Bit-Medium erstellt werden soll.

Robustes Dateisystem (Resilient File System, ReFS)

Sie können in Windows Server 2012 ein Volume mit dem ReFS-Dateisystem formatieren. Dieses Dateisystem bietet im Vergleich zum NTFS-Dateisystem zuverlässigere Verfahren beim Speichern von Daten auf Volumes.

Sie können unter dem **Windows Server 2012** und unter einem **auf WinPE 4 (oder höher) basierenden bootfähigen Medium** ein ReFS-Volume per Backup sichern und wiederherstellen. Eine Größenanpassung von ReFS-Volumes während einer Wiederherstellung wird nicht unterstützt.

Linux-basierte bootfähige Medien und bootfähige Medien, die auf **WinPE vor Version 4.0** basieren, können keine Dateien auf ReFS-Volumes schreiben. Sie können mit solchen Medien daher auch keine Dateien zu einem ReFS-Volume wiederherstellen und ein ReFS-Volume auch nicht als Backup-Ziel auswählen.

Speicherplätze (Storage Spaces)

Unter Windows 8 und Windows Server 2012 ist es möglich, mehrere physikalische Laufwerke zu einem *Speicherpool* (Storage Pool) zu kombinieren. In diesem Speicherpool können wiederum ein oder mehrere logische Datenträger (Disks) erstellt werden, die Speicherplätze (Storage Spaces) genannt werden. Speicherplätze können wie gewöhnliche Laufwerke ebenfalls Volumes haben.

Sie können unter **Windows 8**, unter dem **Windows Server 2012** und unter einem **auf WinPE 4 (oder höher) basierenden Boot-Medium** Backup- und Recovery-Aktionen mit Speicherplätzen durchführen. Unter dem Windows Server 2012 und unter einem auf WinPE 4 (oder höher) basierenden Boot-Medium können Sie außerdem einen Speicherplatz (Storage Space) zu einem herkömmlichen Laufwerk wiederherstellen (und umgekehrt).

Linux-basierte Boot-Medien können keine Speicherplätze erkennen. Sie sichern die zugrundeliegenden Laufwerke aber per Sektor-für-Sektor-Backup. Dasselbe gilt für den **Agenten für ESX(i)** und den **Agenten für Hyper-V.** Falls Sie alle zugrundeliegenden Laufwerke zu den *ursprünglichen* Laufwerken wiederherstellen, werden auch die Speicherplätze (Storage Spaces) wieder neu erstellt.

Datendeduplizierung

Unter Windows Server 2012 können Sie die Datendeduplizierungsfunktion für NTFS-Volumes aktivieren. Datendeduplizierung reduziert den auf dem Volume belegten Speicherplatz, indem doppelt vorhandene Fragemente der Dateien des Volumes nur je einmal gespeichert werden.

Sie können ein Volume, für das die Datendeduplizierung aktiviert ist, auf Laufwerksebene ohne Einschränkungen per Backup sichern und wiederherstellen. Backups auf Dateiebene und Datei-Recovery (einschließlich Datei-Recovery von Laufwerk-Backups) werden nicht unterstützt.

Die Datendeduplierungsfunktion von Windows Server 2012 und die Deduplizierungsfunktion von Acronis Backup & Recovery 11.5 sind eigenständig und ohne Bezug zueinander.

3.11 Kompatibilität mit Verschlüsselungssoftware

Acronis Backup & Recovery 11.5 behält seine komplette Funktionalität, wenn Sie es zusammen mit Verschlüsselungssoftware auf Dateiebene einsetzen.

Verschlüsselungssoftware auf Laufwerksebene verschlüsselt Daten 'on the fly'. Daher sind die entsprechenden, in ein Backup aufgenommenen Daten nicht verschlüsselt. Programme zur Laufwerksverschlüsselung modifizieren häufig wichtige Systembereiche: Boot-Record oder Partitionstabellen oder Dateisystemtabellen. Diese Faktoren haben einen Einfluss auf Backup- und Recovery-Aktionen auf Laufwerksebene sowie auf die Fähigkeit eines wiederhergestellten Systems, zu booten oder auf die Acronis Secure Zone zuzugreifen.

Unter bestimmten Bedingungen ist Acronis Backup & Recovery 11.5 jedoch mit folgenden Programmen zur Laufwerksverschlüsselung kompatibel:

- Microsoft BitLocker-Laufwerksverschlüsselung
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption.

Um zuverlässige Wiederherstellungen auf Laufwerksebene zu garantieren, sollten Sie entsprechenden allgemeinen Regeln sowie den Software-spezifischen Empfehlungen folgen.

Allgemeine Installationsregel

Es wird dringend empfohlen, eine Verschlüsselungssoftware vor der Installation von Acronis Backup & Recovery 11.5 einzurichten.

Verwendung der Acronis Secure Zone

Eine Acronis Secure Zone darf keiner Laufwerksverschlüsselung unterzogen werden. Das ist einzige Art, die Acronis Secure Zone dann zu verwenden:

1. Installieren Sie zuerst die Verschlüsselungssoftware und dann Acronis Backup & Recovery 11.5.
2. Erstellen Sie eine Acronis Secure Zone
3. Schließen Sie die Acronis Secure Zone von der Verschlüsselung des Laufwerks oder seiner Volumes aus.

Allgemeine Backup-Regel

Sie können ein Laufwerk-Backup im Betriebssystem durchführen. Versuchen Sie nicht, das Backup unter Verwendung eines bootfähigen Mediums oder des Acronis Startup Recovery Manager durchzuführen.

Software-spezifische Recovery-Prozeduren

Microsoft BitLocker-Laufwerksverschlüsselung

So stellen Sie ein System wieder her, das per BitLocker verschlüsselt wurde:

1. Booten Sie mit einem bootfähigen Medium.
2. Stellen Sie das System wieder her. Die wiederhergestellten Daten sind unverschlüsselt.
3. Booten Sie das wiederhergestellte System neu.
4. Schalten Sie die BitLocker-Funktion ein.

Falls Sie nur ein Volume eines mehrfach partitionierten Laufwerks wiederherstellen müssen, so tun Sie dies unter dem Betriebssystem. Eine Wiederherstellung mit einem bootfähigen Medium kann dazu führen, dass das wiederhergestellte Volume (die Partition) für Windows nicht mehr erkennbar ist.

McAfee Endpoint Encryption und PGP Whole Disk Encryption

Sie können ein verschlüsseltes System-Volume nur durch Verwendung eines bootfähigen Mediums wiederherstellen.

Falls das wiederhergestellte System nicht mehr bootet, erstellen Sie einen neuen Master Boot Record, wie in folgendem Artikel der Acronis Knowledge Base beschrieben: http://kb.acronis.com/content/1507 und booten Sie dann neu.

3.12 Unterstützung für SNMP

SNMP-Objekte

Acronis Backup & Recovery 11.5 stellt die folgenden Simple Network Management Protocol (SNMP)-Objekte für SNMP-Verwaltungsanwendungen zur Verfügung:

- Typ des Ereignisses

Objekt-Identifier (OID): 1.3.6.1.4.1.24769.100.200.1.0

Syntax: OctetString

Der Wert kann „Information", „Warnung", „Fehler" und „Unbekannt" sein. „Unbekannt" wird nur in der Testnachricht gesendet.

- Textbeschreibung des Ereignisses

  Objekt-Identifier (OID): 1.3.6.1.4.1.24769.100.200.2.0

  Syntax: OctetString

  Der Wert enthält die Textbeschreibung des Ereignisses (identische Darstellung wie in den Meldungen der Ereignisanzeige von Acronis Backup & Recovery 11.5).

Beispiele für Varbind-Werte:

1.3.6.1.4.1.24769.100.200.1.0:Information

1.3.6.1.4.1.24769.100.200.2.0:I0064000B

Unterstützte Aktionen

Acronis Backup & Recovery 11.5 **unterstützt nur TRAP-Aktionen**. Es ist nicht möglich, Acronis Backup & Recovery 11.5 unter Verwendung von GET- und SET-Anforderungen zu verwalten. Das bedeutet, dass Sie einen SNMP-TRAP-Receiver verwenden müssen, um TRAP-Meldungen zu empfangen.

Über die Management Information Base (MIB)

Die MIB-Datei **acronis-abr.mib** befindet sich im Installationsverzeichnis von Acronis Backup & Recovery 11.5. Standardmäßig: %ProgramFiles%\Acronis\BackupAndRecovery unter Windows und /usr/lib/Acronis/BackupAndRecovery unter Linux.

Diese Datei kann von einem MIB-Browser oder einem einfachen Texteditor (wie Notepad oder vi) gelesen werden.

Über die Testnachricht

Sie können bei der Konfiguration von SNMP-Benachrichtigungen eine Testnachricht versenden, um zu überprüfen, ob Ihre Einstellungen richtig sind.

Die Parameter der Testnachricht lauten folgendermaßen:

- Typ des Ereignisses

  OID: 1.3.6.1.4.1.24769.100.200.1.0

  Wert: „Unbekannt"

- Textbeschreibung des Ereignisses

  OID: 1.3.6.1.4.1.24769.100.200.2.0

  Wert: "?00000000"

4 Backup

4.1 Backup jetzt

Verwenden Sie die Funktion **Backup jetzt**, um ein einmaliges Backup mit wenigen einfachen Schritten zu konfigurieren und zu starten. Der Backup-Prozess wird unmittelbar ausgeführt, sobald Sie alle benötigten Schritte durchgeführt und auf **OK** geklickt haben.

Für längerfristige Backup-Strategien, die Planung und Bedingungen einschließen (etwa zeitbedingtes Löschen oder Verschieben von Backups zu anderen Speicherorten), sollten Sie besser die Erstellung eines Backup-Plans erwägen.

Die Konfiguration eines sofortigen Backups gleicht der Erstellung eines Backup-Plans (S. 58) mit folgenden Unterschieden:

- Es gibt keine Optionen zur Planung von Backups oder zur Konfiguration von Aufbewahrungsregeln.
- Eine vereinfachte Benennung der Backup-Dateien (S. 83) wird verwendet, sofern dies vom Backup-Ziel unterstützt wird. Anderenfalls wird die Standard-Backup-Benennung verwendet.

  Folgende Speicherorte unterstützen keine vereinfachte Dateibenennung: verwaltete Depots, Bänder, die Acronis Secure Zone oder der Acronis Online Backup Storage.
- Aufgrund der vereinfachten Dateibenennung kann ein RDX- oder USB-Flash-Laufwerk nur im Modus Wechselmedium (S. 221) verwendet werden.
- Die Möglichkeit zum Konvertieren eines Laufwerk-Backups zu einer virtuellen Maschine steht nicht als Teil der Backup-Aktion zur Verfügung. Sie können die resultierenden Backups aber anschließend konvertieren.

4.2 Erstellung eines Backup-Plans

Bevor Sie Ihren ersten Backup-Plan (S. 486) erstellen, sollten Sie sich mit den grundlegenden Konzepten vertraut machen, die in Acronis Backup & Recovery 11.5 verwendet werden.

Zur Erstellung eines Backup-Plans führen Sie folgende Schritte aus.

Backup-Quelle

Elemente für das Backup (S. 61)

Wählen Sie den zu sichernden Datentyp und spezifizieren Sie die Datenelemente für das Backup. Der Typ der Daten hängt von den auf der Maschine installierten Agenten ab.

Anmeldedaten, Ausschließungen

Klicken Sie auf **Anmeldedaten, Ausschließungen anzeigen**, um auf diese Einstellung zugreifen zu können.

Anmeldedaten (S. 63)

Stellen Sie Anmeldedaten für die Quelldaten zur Verfügung, falls das Konto des Plans keine Zugriffserlaubnis für die Daten hat.

Ausschließungen (S. 63)

Definieren Sie Ausschließungen für spezifische Datei-Typen, die Sie nicht mit ins Backup aufnehmen wollen.

Backup-Ziel

Speicherort (S. 65)

Spezifizieren Sie einen Pfad zu dem Ort, wo das Backup-Archiv gespeichert wird, sowie den Namen des Archivs. Der Archivname muss innerhalb des Zielordners eindeutig sein. Anderenfalls werden die Backups des neu erstellten Backup-Plans bei einem bereits existierenden Archiv hinterlegt, das zu einem anderen Backup-Plan gehört. Der vorgegebene Archivname ist Archive(N), wobei N die fortlaufende Nummer des Archivs im gewählten Speicherort ist.

Wählen Sie den Modus, in dem das Wechsellaufwerk verwendet wird (S. 221)

Sollte es sich beim angegebenen Speicherort um ein RDX- oder USB-Flash-Laufwerk handeln, dann wählen Sie den Gerätemodus: **Wechselmedium** oder **Eingebautes Laufwerk**.

Benennung der Backup-Datei, Anmeldedaten, Archivkommentare

Klicken Sie auf **Benennung der Backup-Datei, Anmeldedaten, Archivkommentare anzeigen**, um Zugriff auf diese Einstellungen zu erhalten.

Dateibenennung (S. 83)

[Optional] Aktivieren Sie das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen, wie in Acronis True Image Echo, anstelle automatisch generierter Namen**, falls Sie für die Backups des Archivs eine vereinfachte Dateibenennung verwenden wollen.

Nicht verfügbar, wenn Sie Backups zu einem verwalteten Depot, auf Band, zu einer Acronis Secure Zone oder dem Acronis Online Backup Storage durchführen. Beim Backup zu einem RDX- oder USB-Flash-Laufwerk wird das Dateibenennungsschema durch den Wechsellaufwerkmodus (S. 221) bestimmt.

Anmeldedaten (S. 68)

[Optional] Stellen Sie Anmeldedaten für den Speicherort zur Verfügung, falls das Konto des Plans keine Zugriffserlaubnis für den Ort hat.

Archiv-Kommentare

[Optional] Tragen Sie Kommentare für das Archiv ein.

Single-Pass-Laufwerk- und Anwendungs-Backup (S. 350)

Gilt nur für Maschinen, die über eine Lizenz für Single-Pass-Backup verfügen.

Spezifizieren Sie für Single-Pass-Laufwerk- und Anwendungs-Backups geltende Einstellungen.

Art des Backups

Backup-Schema (S. 69)

Spezifizieren Sie, wann und wie oft Ihre Daten gesichert werden sollen, definieren Sie, wie lange die erzeugten Backup-Archive im gewählten Speicherort aufbewahrt werden sollen; erstellen Sie einen Zeitplan zur Bereinigung der Archive (siehe den nachfolgenden Abschnitt 'Replikations- und Aufbewahrungseinstellungen').

Replikations- und Aufbewahrungseinstellungen (S. 104)

Nicht verfügbar für Wechselmedien oder wenn die vereinfachte Benennung für Backup-Dateien (S. 83) *gewählt wurde.*

Definieren Sie, ob die Backups zu einem anderen Speicherort kopiert (repliziert) werden sollen – und ob sie gemäß den Aufbewahrungsregeln verschoben oder gelöscht werden sollen. Die verfügbaren Einstellungen hängen vom Backup-Schema ab.

2. Speicherort

[Optional] Aktivieren Sie zur Einrichtung einer Backup-Replikation das Kontrollkästchen **Neu erstelltes Backup zu einem anderen Speicherort replizieren**. Zu weiteren Informationen über Backup-Replikation siehe 'Replikation von Backups einrichten (S. 106)'.

Validierung, zu virtueller Maschine konvertieren

Klicken Sie auf **Anzeigen: Validierung, zu virtueller Maschine konvertieren**, um Zugriff auf diese Einstellungen zu erhalten.

Validierungszeitpunkt (S. 79)

[Optional] Definieren Sie, abhängig vom gewählten Backup-Schema, wann und wie oft eine Validierung durchzuführen ist und ob das komplette Archiv oder nur das letzte Backup im Archiv validiert werden soll.

Zu virtueller Maschine konvertieren (S. 192)

[Optional] Gilt für: Laufwerk/Volume-Backups, die Backups kompletter virtueller Maschinen oder die Volumes einer virtuellen Maschine.

Richten Sie die regelmäßige Konvertierung eines Laufwerk- oder Volume-Backups zu einer virtuellen Maschine ein.

Plan-Parameter

Plan-Name

[Optional] Geben Sie einen eindeutigen Namen für den Backup-Plan ein. Ein bewusst gewählter Name macht es leichter, diesen Plan zu identifizieren.

Backup-Optionen

[Optional] Konfigurieren Sie Parameter für eine Backup-Aktion, wie zum Beispiel die Befehle vor bzw. nach dem Backup, die maximale Bandbreite im Netzwerk, die dem Backup zugeteilt wird, oder den Komprimierungsgrad für das Backup-Archiv. Sofern Sie in diesem Abschnitt nichts tun, werden die Standardwerte (S. 114) verwendet.

Wird irgendeine Einstellung gegenüber dem Standardwert geändert, so wird der neue Wert in einer Zeile angezeigt. Der Einstellungsstatus ändert sich von **Standard** zu **Auf Standard zurücksetzen**. Sollten Sie die Einstellung erneut ändern, so wird die Zeile ebenfalls den neuen Wert anzeigen, sofern er nicht dem Standardwert entspricht. Wenn der Standardwert eingestellt wird, verschwindet die Zeile. Sie sehen daher in diesem Abschnitt immer nur die Einstellungen, die von den Standardwerten abweichen.

Um alle Einstellungen auf Standardwerte zurückzusetzen, klicken Sie auf **Auf Standard zurücksetzen**.

Anmeldedaten des Plans, Kommentare, Bezeichnung

Klicken Sie auf **Anmeldedaten des Plans, Kommentare, Bezeichnung anzeigen**, um auf diese Einstellung zugreifen zu können.

Anmeldedaten des Plans (S. 80)

[Optional] Spezifizieren Sie die Anmeldedaten, unter denen der Plan laufen soll.

Kommentare

[Optional] Geben Sie eine Beschreibung bzw. einen Kommentar für den Backup-Plan ein.

Bezeichnung (S. 80)

[Optional] Geben Sie für die zu sichernde Maschine eine Textbezeichnung ein. Diese Bezeichnung kann verwendet werden, um die Maschine in verschiedenen Szenarien zu identifizieren.

Nachdem Sie alle notwendigen Schritte durchgeführt haben, klicken Sie auf **OK**, um den Backup-Plan zu erstellen.

Danach kann es sein, dass Sie zur Eingabe eines Kennworts (S. 83) aufgefordert werden.

Sie können auf den von Ihnen erstellten Plan in der Ansicht **Backup-Pläne und Tasks** (S. 360) zur Untersuchung und Verwaltung zugreifen.

4.2.1 Daten für ein Backup auswählen

So wählen Sie Daten für ein Backup aus

1. Bestimmen Sie im Abschnitt **Daten für das Backup** den Typ derjenigen Daten, die Sie sichern wollen. Die Liste der verfügbaren Datentypen hängt von den Agenten ab, die auf der Maschine laufen und den Lizenztypen:

   Laufwerke/Volumes

   Sie müssen Benutzerrechte als Administrator oder Sicherungs-Operator haben, um diese Daten sichern zu können.

   Wählen Sie diese Option zum Backup:

   - Kompletter physikalischer Maschinen oder einzelner Laufwerke bzw. Volumes von diesen, falls der Acronis Backup & Recovery 11.5 Agent für Windows oder der Acronis Backup & Recovery 11.5 Agent für Linux installiert ist.

     Ein Laufwerk-Backup ermöglicht Ihnen, ein komplettes System auch bei schwerer Datenbeschädigung oder Hardware-Ausfall wiederherzustellen. Sie können außerdem einzelne Dateien und Ordner wiederherstellen. Diese Backup-Prozedur ist schneller als ein einfaches Kopieren von Dateien und kann Backup-Prozesse beim Sichern großer Datenmengen signifikant beschleunigen.
   - Microsoft SQL-Datenbanken mithilfe von Single-Pass-Laufwerk- und Anwendungs-Backup, falls der Acronis Backup & Recovery 11.5 Agent für Microsoft SQL Server (Single-Pass) installiert ist.

     Der Agent für SQL (Single-Pass) ermöglicht Ihnen, applikationskonforme Laufwerk-Backups zu erstellen und Microsoft SQL-Datenbanken von solchen Backups wiederherzustellen. Weitere Informationen finden Sie im Abschnitt 'Microsoft SQL Server schьtzen... (S. 345)'.
   - Microsoft Active Directory-Daten mithilfe von Single-Pass-Laufwerk- und Anwendungs-Backup, falls der Acronis Backup & Recovery 11.5 Agent für Microsoft SQL Server (Single-Pass) installiert ist.

     Der Agent für Active Directory (Single-Pass) ermöglicht Ihnen, applikationskonforme Laufwerk-Backups zu erstellen und Microsoft Active Directory-Daten von solchen Backups wiederherzustellen. Weitere Informationen finden Sie im Abschnitt 'Microsoft Active Directory schьtzen... (S. 356)'.

   Ordner/Dateien

   Ist verfügbar, wenn der Acronis Backup & Recovery 11.5 Agent für Windows oder der Acronis Backup & Recovery 11.5 Agent für Linux installiert ist.

   Aktivieren Sie diese Option, um spezifische Dateien und Ordner zu sichern.

   Ein dateibasiertes Backup ist zur Wiederherstellung eines Betriebssystems nicht ausreichend geeignet. Verwenden Sie ein Datei-Backup, wenn Sie nur bestimmte Daten (beispielsweise ein aktuelles Projekt) sicher bewahren wollen. Das reduziert die Archivgröße und spart so Speicherplatz.

Um Ihr Betriebssystem mit all seinen Einstellungen und Anwendungsprogrammen wiederherstellen zu können, müssen Sie ein Laufwerk-Backup durchführen.

Virtuelle Maschinen

Ist verfügbar, wenn der Acronis Backup & Recovery 11.5 Agent für ESX(i) oder der Acronis Backup & Recovery 11.5 Agent für Hyper-V installiert ist.

Verwenden Sie diese Option, um auf einem Virtualisierungsserver liegende virtuelle Maschinen komplett oder nur deren Laufwerke bzw. Volumes zu sichern.

Das Backup einer kompletten virtuellen Maschine (oder ihrer Laufwerke bzw. Volumes) ergibt standardmäßig ein Laufwerk-Backup (S. 489). Ein solches Backup speichert zudem auch die Konfiguration der virtuellen Maschine. Diese Konfiguration wird Ihnen als Standard vorgeschlagen, wenn Sie den Backup-Inhalt zu einer neuen virtuellen Maschine wiederherstellen wollen. Zu weiteren Informationen über die Sicherung virtueller Maschinen siehe den Abschnitt 'Backups von virtuellen Maschinen'.

Microsoft Exchange-Informationsspeicher

Ist verfügbar, falls der Acronis Backup & Recovery 11.5 Agent für Microsoft Exchange Server installiert ist.

Wählen Sie diese Option, um den Informationsspeicher, einzelne Speichergruppen oder Datenbanken von Microsoft Exchange-Servern per Backup zu sichern. Im Fall eines Desasters sind Sie in der Lage, verlorene bzw. beschädigte Datenbanken oder Speichergruppen wiederherzustellen. Sie können einzelne Postfächer, Öffentliche Ordner, einzelne E-Mails, Kontakte, Kalenderereignisse und andere Elemente wiederherstellen.

Um Exchange-Daten per Backup sichern zu können, ist ein Domain-Benutzerkonto mit administrativen Berechtigungen auf dem Exchange-Server erforderlich. In einem Cluster muss das Konto über administrative Berechtigungen auf jedem der Cluster-Knoten verfügen.

Zu weiteren Informationen über die Sicherung von Microsoft-Exchange-Daten siehe 'Backups von Microsoft Exchange-Server-Daten'.

Microsoft Exchange-Postfächer

Ist verfügbar, falls der Acronis Backup & Recovery 11.5 Agent für Microsoft Exchange Server installiert ist.

Wählen Sie diese Option, um einzelne Postfächer und Öffentliche Ordner zu sichern, ohne ein Backup der kompletten Microsoft Exchange-Daten durchzuführen. Sie können durch Verwendung von Ausschlussfiltern festlegen, dass bestimmte Elemente bei den Postfach-Backups übersprungen werden.

Um Exchange-Daten per Backup sichern zu können, ist ein Domain-Benutzerkonto mit administrativen Berechtigungen auf dem Exchange-Server erforderlich. In einem Cluster muss das Konto über administrative Berechtigungen auf jedem der Cluster-Knoten verfügen.

Zu weiteren Informationen über die Sicherung von Microsoft-Exchange-Daten siehe 'Backups von Microsoft Exchange-Server-Daten'.

2. Wählen Sie im Verzeichnisbaum unter dem Bereich **Daten für das Backup** die zu sichernden Elemente.

   Um alle auf einer Maschine präsenten Elemente des gewählten Datentyps zu sichern, aktivieren Sie das Kontrollkästchen neben der Maschine. Um einzelne Datenelemente zu sichern, müssen Sie die Maschine erweitern und die Kontrollkästchen neben den gewünschten Elementen aktivieren.

   Hinweise für Laufwerke/Volumes

   - Falls Betriebssystem und Boot-Loader auf unterschiedlichen Volumes liegen, nehmen Sie immer beide mit in das Backup auf. Diese Laufwerke müssen auch zusammen

wiederhergestellt werden, da anderenfalls ein hohes Risiko besteht, dass das Betriebssystem nicht mehr startet.

- Hinweis für Linux-Benutzer: Logische Volumes und MD-Geräte werden unter **Dynamische Volumes** angezeigt. Zu weiteren Informationen über das Backup solcher Volumes und Geräte siehe 'Backup und Recovery von logischen Volumes und MD-Gerдten (Linux) (S. 46)'.
- Hinweis für Linux-Benutzer: Es wird empfohlen, dass Sie vor dem Backup alle Volumes trennen, die kein Journaling-Dateisystem – wie z.B. ext2 – enthalten. Anderenfalls könnten diese Volumes bei einer Wiederherstellung beschädigte Dateien enthalten; eine Wiederherstellung dieser Volumes bei gleichzeitiger Größenänderung könnte fehlschlagen.

Hinweise für Virtuelle Maschinen

- Eine Sicherung kompletter virtueller Maschinen ist praktisch, wenn kleine (bezogen auf die virtuelle Laufwerksgröße), aber zahlreiche Legacy-Server vorhanden sind, wie sie aus Systemen zur Server-Auslastung resultieren (Workload-Konsolidierung). Für jede Maschine wird ein separates Archiv erstellt.
- Eine Sicherung einzelner Laufwerke oder Volumes einer virtuellen Maschine ist praktisch, wenn ein Betriebssystem und Anwendungen (etwa ein Datenbank-Server) auf einem virtuellen Laufwerk liegen, während die Daten (etwa eine Datenbank) auf einem physikalischen, derselben Maschine hinzugefügten Laufwerk mit hoher Kapazität gespeichert sind. Sie können für das virtuelle Laufwerk und den physikalischen Speicher unterschiedliche Backup-Strategien verwenden.

3. Klicken Sie auf **OK**, wenn Sie die Daten für das Backup spezifiziert haben.

4.2.2 Anmeldedaten der Quelle

Spezifizieren Sie die Anmeldedaten, um auf die zu sichernden Daten zugreifen zu können.

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Anmeldedaten des Plans verwenden**

     Das Programm greift auf die Quelldaten mit den Anmeldedaten des Backup-Plan-Kontos zu, wie sie im Abschnitt **Plan-Parameter** spezifiziert wurden.
   - **Folgende Anmeldedaten verwenden**

     Das Programm greift auf die Quelldaten unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu.

     Verwenden Sie diese Option, sofern das Konto des Plans keine Zugriffserlaubnis für die Daten hat.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
     - **Kennwort bestätigen**. Geben Sie das Kennwort erneut ein.
2. Klicken Sie auf **OK**.

4.2.3 Ausschluss von Quelldateien

Diese Option ist für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Option ist nur für Backups auf *Laufwerksebene* von NTFS-, FAT-, Ext3- und Ext4-Dateisystemen wirksam. Diese Option ist bei Backups auf *Dateiebene* für alle unterstützten Dateisysteme wirksam.

Diese Option definiert, welche Dateien und Ordner während des Backup-Prozesses übersprungen und so von der Liste der zu sichernden Elemente ausgeschlossen werden.

Hinweis: *Ausschließungen überschreiben eine Auswahl von Datenelementen, die per Backup gesichert werden sollen. Falls Sie beispielsweise festlegen, dass die Datei 'MeineDatei.tmp' per Backup gesichert werden soll und Sie aber zudem alle .tmp-Dateien ausschließen, dann wird 'MeineDatei.tmp' nicht mitgesichert.*

Setzen Sie folgende Parameter, um die auszuschließenden Dateien und Ordner zu spezifizieren.

Alle versteckten Dateien und Ordner ausschließen

Aktivieren Sie dieses Kontrollkästchen, um Dateien und Ordner zu überspringen, die mit dem Attribut **Versteckt** gekennzeichnet sind (bei von Windows unterstützten Dateisystemen) – oder die mit einem Punkt (.) beginnen (bei Dateisystemen unter Linux wie Ext2 und Ext3). Bei Ordnern mit dem Attribut 'Versteckt' wird der gesamte Inhalt ausgeschlossen (einschließlich solcher Dateien, die nicht versteckt sind).

Ausschluss aller Systemdateien und -ordner

Diese Option ist nur für Dateisysteme wirksam, die von Windows unterstützt werden. Aktivieren Sie dieses Kontrollkästchen, um alle Dateien und Ordner mit dem Attribut **System** zu überspringen. Bei Ordnern mit dem Attribut **System** wird der gesamte Inhalt ausgeschlossen (einschließlich solcher Dateien, die nicht mit dem Attribut **System** gekennzeichnet sind).

Tipp: *Sie können die Attribute von Dateien oder Ordnern über ihre Datei-/Ordner-Eigenschaften einsehen -— oder mit dem Kommandozeilenbefehl* ***attrib****. Weitere Informationen finden Sie im Hilfe und Support-Center von Windows.*

Dateien ausschließen, die folgende Kriterien erfüllen

Aktivieren Sie dieses Kontrollkästchen, um alle Dateien und Ordner zu überspringen, die einem der Kriterien entsprechen. Verwenden Sie die Schaltflächen **Hinzufügen**, **Bearbeiten**, **Entfernen** und **Alle entfernen**, um die Liste der Kriterien zu verwalten.

Bei den Kriterien wird *nicht* auf Groß-/Kleinschreibung geachtet (in Windows und Linux). Falls Sie beispielsweise festlegen, dass alle .tmp-Dateien und der Ordner C:\Temp ausgeschlossen werden sollen, dann werden auch alle .Tmp-Dateien, alle .TMP-Dateien und der Ordner C:\TEMP ausgeschlossen.

Kriterium: vollständiger Pfad

Spezifizieren Sie den vollständigen Pfad zu der Datei oder dem Ordner, indem Sie mit dem Laufwerksbuchstaben (bei Backups unter Windows) oder dem Stammverzeichnis (bei Backups unter Linux) beginnen.

Sie können unter Windows und Linux im Datei- bzw. Ordnerpfad einen normalen Schrägstrich (Slash) verwenden (wie bei **C:/Temp** und **C:/Temp/Datei.tmp**). Unter Windows können Sie auch den üblichen, nach links geneigten Schrägstrich (Backslash) verwenden (wie bei **C:\Temp** und **C:\Temp\Datei.tmp**).

Beim Verwenden eines Windows-typischen bootfähigen Mediums kann ein Volume einen anderen Laufwerksbuchstaben als unter Windows haben. Weitere Informationen finden Sie im Abschnitt 'Mit bootfдhigen Medien arbeiten (S. 294)'.

Kriterium: name

Spezifizieren Sie den Namen der Datei oder des Ordners, wie etwa 'Dokument.txt'. Alle Dateien und Ordner mit diesem Namen werden ausgeschlossen.

Platzhalterzeichen (Wildcards)

Sie können ein oder mehrere Platzhalterzeichen (* und ?) in dem Kriterium verwenden. Diese Zeichen können innerhalb des vollständigen Pfades und im Namen der Datei oder des Ordners verwendet werden.

Das Asterisk (*) ersetzt null bis mehrere Zeichen in einem Dateinamen. So beinhaltet beispielsweise das Kriterium 'Doc*.txt' Dateien wie 'Doc.txt' und 'Document.txt'.

Das Fragezeichen (?) steht für exakt ein Zeichen in einem Dateinamen. Beispielsweise beinhaltet das Kriterium 'Doc?.txt' Dateien wie 'Doc1.txt' und 'Docs.txt' – aber nicht 'Doc.txt' oder 'Doc11.txt'.

Beispiele für Ausschließungen

Kriterium	Beispiel	Beschreibung
	Windows und Linux	
Per Name	F.log F	Schließt alle Dateien namens 'F.log' aus Schließt alle Ordner namens 'F' aus
Per Maske (*)	*.log F*	Schließt alle Dateien mit der Erweiterung „.log“ aus Schließt alle Dateien und Ordner aus, deren Namen mit „F“ beginnen (etwa die Ordner F, F1 und die Dateien F.log, F1.log)
Per Maske (?)	F???.log	Schließt alle .log-Dateien aus, deren Namen am Ende vier Zeichen enthalten und mit „F“ beginnen
	Windows	
Per Dateipfad	C:\Finanzen\F.log	Schließt eine Datei aus, die 'F.log' heißt und im Ordner 'C:\Finanzen' vorliegt
Per Ordnerpfad	C:\Finanzen\F *oder* C:\Finanzen\F\	Schließt den Ordner 'C:\Finanzen\F' aus (stellen Sie sicher, dass Sie den vollständigen Pfad angeben, beginnend mit einem Laufwerksbuchstaben)
	Linux	
Per Dateipfad	/home/user/Finanzen/F.log	Schließt eine Datei aus, die 'F.log' heißt und im Ordner (Verzeichnis) '/home/user/Finanzen' vorliegt
Per Ordnerpfad	/home/user/Finanzen *oder* /home/user/Finanzen/	Schließt den Ordner (Verzeichnis) '/home/user/Finanzen' aus

4.2.4 Auswahl der Backup-Speicherortes

Spezifizieren Sie, wo das Archiv gespeichert werden soll.

1. Ziel wählen

Tragen Sie den vollständigen Pfad zum Zielort in das Feld **Pfad** ein oder wählen Sie das gewünschte Ziel aus dem Verzeichnisbaum (wie im Abschnitt 'Auswahl der Backup-Zielorte (S. 66)' beschrieben.

2. Archiv-Tabelle verwenden

Die Tabelle zeigt für jeden gewählten Speicherort die Namen dort enthaltener Archive an, um Ihnen die Wahl des richtigen Ziels zu erleichtern. Während Sie den Inhalt eines Speicherorts untersuchen, können Archive durch einen anderen Benutzer oder das Programm (auf Basis geplanter Aktionen) hinzugefügt, gelöscht oder modifiziert werden. Verwenden Sie die Schaltfläche **Aktualisieren**, um die Liste der Archive neu aufzubauen.

3. Das neue Archiv benennen

Sobald Sie den Zielort für das Archiv gewählt haben, erstellt das Programm einen Namen für das neue Archiv und zeigt diesen im Feld **Name** an. Der Name sieht üblicherweise aus wie *Archiv(N)*, wobei *N* eine fortlaufende Nummer ist. Der generierte Name ist innerhalb des gewählten Speicherortes eindeutig. Wenn Sie mit dem automatisch generierten Namen einverstanden sind, dann klicken Sie auf **OK**. Geben Sie anderenfalls einen eindeutigen Namen ein.

Sollte der automatisch generierte Name wie *[Maschinenname]_Archiv(N)* aussehen, dann sind im Namen Variablen enthalten. Das kann der Fall sein, wenn Sie eine virtuelle Maschine zum Backup ausgewählt haben. Die Bezeichnung *[Maschinenname]* steht für den Namen der jeweiligen virtuellen Maschine. Sie können dem Namen Suffixe anhängen, aber löschen Sie nie die Variablen, da jede virtuelle Maschine in ein separates Archiv mit eindeutigem Namen gesichert werden muss.

Backup zu einem existierenden Archiv

Sie können einen Backup-Plan so konfigurieren, dass das Backup zu einem existierenden Archiv erfolgt. Zur Umsetzung wählen Sie das Archiv in der Tabelle oder geben die entsprechende Bezeichnung in das Feld **Name** ein. Sollte das Archiv mit einem Kennwort geschützt sein, wird das Programm in einem Pop-up-Fenster danach fragen.

Durch Wahl des existierenden Archivs erzeugen Sie eine Interaktion mit einem anderen Backup-Plan, der das Archiv ebenfalls verwendet. Das ist kein Problem, falls der andere unterbrochen wurde. Sie sollten im Allgemeinen jedoch folgender Regel folgen: „Ein Backup-Plan – ein Archiv“. Das Gegenteil zu tun, behindert das Programm nicht in seiner Funktion, ist aber unpraktisch bzw. uneffizient, mit Ausnahme einiger Spezialfälle.

Warum zwei oder mehr Backup-Pläne nicht in dasselbe Archiv sichern sollten

1. Wenn Sie unterschiedliche Quellen per Backup in dasselbe Archiv sichern, führt das zu schwierig handhabbaren Archiven. Wenn es darauf ankommt, eine wichtige Wiederherstellung durchzuführen, zählt jede Sekunde; Sie könnten sich in so einer Situation leicht im Inhalt des Archivs 'verlieren'.

   Mit demselben Archiv arbeitende Backup-Pläne sollten auch dieselben Daten-Elemente sichern (z.B. zwei Pläne, die Laufwerk C: sichern).

2. Werden auf ein Archiv multiple Aufbewahrungsregeln angewendet, so macht dies den Inhalt des Archivs unkalkulierbar. Da jede Regel auf das gesamte Archiv angewendet wird, kann es leicht passieren, dass Backups, die zu einem Backup-Plan gehören, zusammen mit Backups gelöscht werden, die zu einem anderen Plan gehören. Sie sollten kein klassisches Verhalten der Backup-Schemata GVS und Türme von Hanoi erwarten.

   Normalerweise sollte jeder komplexe Backup-Plan in 'eigene' Archive sichern.

4.2.4.1 Auswahl der Backup-Zielorte

Acronis Backup & Recovery 11.5 ermöglicht Ihnen, Backups zu verschiedenen physikalischen Speicherorten/-geräten (Storages) zu sichern.

Ziel	Details
Online Backup Storage	Klicken Sie zur Speicherung von Backups auf dem Acronis Online Backup Storage auf **Anmelden**, geben Sie anschließend die Anmeldedaten zum Zugriff auf den Online Storage ein. Erweitern Sie dann die Gruppe **Online Backup Storage** und wählen Sie das Konto. Bevor Sie Ihre Backups auf dem Online Storage sichern können, müssen Sie für den Online Backup Service ein Abonnement kaufen (S. 475) und das Abonnement auf der zu sichernden Maschine aktivieren (S. 477). Die Online Backup-Funktion steht unter Linux und bootfähigen Medien nicht zur Verfügung. Online Backups von Microsoft Exchange-Server-Daten mit dem Agenten für Exchange sind nicht möglich. ***Hinweis:*** *Acronis Backup & Recovery Online ist möglicherweise in Ihrer Region nicht verfügbar. Zu weiteren Informationen klicken Sie hier: http://www.acronis.de/my/backup-recovery-online/*
Persönlich	Um Daten zu einem persönlichen Depot sichern zu können, erweitern Sie die Gruppe **Depots** und klicken auf das Depot. Die Acronis Secure Zone wird als persönliches Depot betrachtet, das für alle Benutzer verfügbar ist, die sich an diesem System anmelden können.
Zentral	Um Daten zu einem zentralen Depot sichern zu können, müssen Sie die Gruppe **Depots** erweitern und dann das entsprechende Depot auswählen.
Maschine	Lokale Maschine
Lokale Ordner	Um Daten zu einem lokalen Ordner einer Maschine sichern zu können, müssen Sie die Gruppe **<Maschinenname>** erweitern und dann den gewünschten Ordner auswählen.
CD, DVD, BD	Um Daten auf optische Medien wie CDs, DVDs oder Blu-ray-Medien (BD) sichern zu können, müssen Sie die Gruppe **<Maschinenname>** erweitern und das gewünschte Laufwerk auswählen.
RDX, USB	Um Daten auf RDX- oder USB-Flash-Laufwerke sichern zu können, müssen Sie die Gruppe **<Maschinenname>** erweitern und das gewünschte Laufwerk auswählen. Weitere Informationen über die Verwendung dieser Laufwerke finden Sie im Abschnitt 'Wechsellaufwerke (S. 221)'.
Bandgerät	Um Daten zu einem lokal angeschlossenen Bandgerät sichern zu können, erweitern Sie die Gruppe **<Maschinename>** und klicken dann auf das gewünschte Gerät. In den Standalone-Editionen von Acronis Backup & Recovery 11.5 stehen Bandgeräte nur zur Verfügung, wenn Sie ein Upgrade von Acronis Backup & Recovery 10 durchgeführt haben. Zu weiteren Informationen über die Verwendung von Bändern siehe den Abschnitt 'Bandgerдte (S. 223).
Netzwerkordner	Um Daten zu einem Netzwerkordner sichern zu können, müssen Sie die Gruppe **Netzwerkordner** erweitern, die gewünschte Netzwerkmaschine auswählen und dann auf den freigegebenen Ordner klicken. Werden Anmeldedaten zum Zugriff auf die Netzwerkfreigabe benötigt, so wird das Programm diese erfragen. ***Hinweis für Linux-Benutzer:*** *Um eine CIFS-Netzfreigabe (Common Internet File System) anzugeben, die zu einem Mount-Punkt wie z.B.* ***/mnt/freigabe****, wählen Sie diesen Mount-Punkt statt der Netzfreigabe aus.*

Ziel	Details
FTP, SFTP	Für Daten über FTP oder SFTP sichern zu können, geben Sie den Namen oder die Adresse des entsprechenden Servers wie folgt in das Feld **Pfad** ein: **ftp://ftp-server:port-nummer** oder **sftp://sftp-server:port-nummer** Verwenden Sie folgende Schreibweise, um eine FTP-Verbindung im aktiven Modus aufzubauen: **aftp://ftp-server:port-nummer** Wenn Sie die Port-Nummer nicht angeben, wird Port 21 für FTP benutzt und Port 22 für SFTP. Nach Eingabe der Anmeldedaten sind die Ordner auf dem Server verfügbar. Klicken Sie auf den passenden Ordner auf dem Server. Sie können auf den Server auch als anonymer Benutzer zugreifen, wenn der Server einen solchen Zugang ermöglicht. Dafür klicken Sie auf **Anonymen Zugang benutzen** anstelle der Eingabe von Anmeldedaten. ***Anmerkung**: Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Klartext über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Packet-Sniffer abgefangen werden.*
Storage Nodes	Wenn Sie Daten zu einem Storage Node sichern müssen, der nicht auf dem Management Server registriert ist, oder wenn Sie auf einer Maschine arbeiten, die Sie mit einem bootfähigen Medium gestartet haben: ▪ Um auf ein verwaltetes Depot zuzugreifen, geben Sie im Feld **Pfad** ein: **bsp://knoten_adresse/depot_name/** ▪ Um auf ein zentrales, nicht verwaltetes Depot zuzugreifen, tragen Sie den vollen Pfad zum Ordner des Depots ein.
NFS-Laufwerke	Um Daten per Backup zu einer NFS-Freigabe sichern zu können, erweitern Sie die Gruppe **NFS-Laufwerke** und klicken Sie auf den entsprechenden Ordner. Nur unter Linux und unter Linux-basierten bootfähigen Medien verfügbar.

4.2.5 Zugriff auf die Anmeldedaten für den Speicherort des Archivs

Spezifizieren Sie die Anmeldedaten, die für den Zugriff auf den Ort notwendig sind, an dem das Backup-Archiv gespeichert wird. Der Benutzer, dessen Name angegeben wird, wird als Besitzer des Archivs betrachtet.

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Anmeldedaten des Plans verwenden**

     Das Programm greift auf die Quelldaten mit den Anmeldedaten des Backup-Plan-Kontos zu, wie sie im Abschnitt **Plan-Parameter** spezifiziert wurden.
   - **Folgende Anmeldedaten verwenden**

     Das Programm greift auf die Quelldaten unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu.

     Verwenden Sie diese Option, sofern das Konto des Plans keine Zugriffsberechtigungen für den Speicherort hat. Es ist möglich, dass Sie für eine Netzwerkfreigabe oder ein Storage Node-Depot noch weitere Anmeldedaten brauchen.

Spezifizieren Sie:

- **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
- **Kennwort**. Das Kennwort für das Konto.
- **Kennwort bestätigen**. Geben Sie das Kennwort erneut ein.

2. Klicken Sie auf **OK**.

Warnung: *Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.*

4.2.6 Backup-Schemata

Wählen Sie eins der verfügbaren Backup-Schemata:

- **Einfach** – um zu planen, wann und wie oft die Daten gesichert werden und Aufbewahrungsregeln zu spezifizieren.
- **Großvater-Vater-Sohn** – um das Großvater-Vater-Sohn-Backup-Schema zu verwenden. Das Schema erlaubt es nicht, dass Daten mehr als einmal pro Tag gesichert werden. Sie bestimmen den Wochentag, an dem das tägliche Backup ausgeführt wird und wählen von diesen Tagen noch einen Tag zum wöchentlichen und monatlichen Backup. Dann definieren Sie die Aufbewahrungsregeln für die täglichen (entspricht dem „Sohn“), wöchentlichen („Vater“) und monatlichen („Großvater“) Backups. Abgelaufene Backups werden automatisch gelöscht.
- **Türme von Hanoi** – zur Verwendung des Backup-Schema 'Türme von Hanoi'. Mit diesem Schema können Sie planen, wann und wie oft Backups (Sitzungen) erfolgen sollen und eine entsprechende Zahl von Backup-Levels zu bestimmen (bis zu 16). Die Daten können dabei mehrmals pro Tag gesichert werden. Indem Sie die Backup-Planung aufstellen und die Backup-Level wählen, erhalten Sie automatisch die Roll-back-Periode – die garantierte Zahl von Sitzungen, zu der Sie jederzeit zurückgehen können. Der automatische Bereinigungsmechanismus hält die benötigte Roll-back-Periode aufrecht, indem er die abgelaufenen Backups löscht und von jedem Level die neusten Backups behält.
- **Benutzerdefiniert** – um ein benutzerdefiniertes Schema zu erstellen, das Ihnen ermöglicht, eine Backup-Strategie in der für Ihr Unternehmen benötigten Art aufzustellen: Spezifizieren Sie multiple Zeit-/Ereignis-Pläne für verschiedene Backup-Typen, fügen Sie Bedingungen hinzu und definieren Sie die Aufbewahrungsregeln.
- **Manueller Start** – um einen Backup-Task zum manuellen Start zu erstellen.
- **Initial Seeding** – zum lokalen Speichern eines Voll-Backups, das später auf dem Acronis Online Backup Storage hinterlegt wird.

Hinweis für Microsoft Exchange-Benutzer: *Weitere Informationen über Backup-Schemata, die beim Backup von Exchange-Datenbanken, Speichergruppen oder Postfächern verwendet werden, finden Sie im Abschnitt 'Backup-Schemata' der Dokumentation 'Backups von Microsoft Exchange-Server-Daten'.*

4.2.6.1 Schema 'Einfach'

Mit dem Backup-Schema 'Einfach' planen Sie nur, wann und wie oft die Daten gesichert werden sollen. Andere Schritte sind optional.

Zur Einrichtung des Backup-Schemas 'Einfach' spezifizieren Sie die passenden Einstellungen wie folgt:

Planung

Legen Sie fest, wann und wie oft die Daten gesichert werden sollen. Siehe den Abschnitt Planung (S. 89), um mehr über das Einrichten von Zeit/-Ereignis-Planungen zu lernen.

Aufbewahrungsregeln

Spezifizieren Sie, wie lange Backups im Speicherort aufbewahrt werden sollen und ob sie danach verschoben oder gelöscht werden sollen. Die Aufbewahrungsregeln werden angewendet, wenn ein Backup erstellt wird. Standardmäßig ist die Option **Backups unbegrenzt behalten** aktiviert, was bedeutet, dass keine Backups automatisch gelöscht werden. Zu weiteren Informationen über Aufbewahrungsregeln siehe 'Aufbewahrungsregeln von Backups einstellen (S. 107)'.

Backup-Typ

Klicken Sie auf **Anzeigen: Backup-Typ, Validierung, zu virtueller Maschine konvertieren**, um Zugriff auf diese Einstellung zu erhalten.

Bestimmen Sie den Backup-Typ.

- **Vollständig**. Standardmäßig für alle Backup-Speicherorte (mit Ausnahme des Acronis Online Backup Storages) vorausgewählt.
- **Inkrementell**. Beim ersten Mal wird immer ein Voll-Backup erstellt. Die nachfolgenden Backups werden inkrementell. Als einziger Backup-Typ für den Acronis Online Backup Storage ausgewählt.

__Anmerkung__: Wenn der Backup-Typ __Inkrementell__ zusammen mit den Aufbewahrungsregeln ausgewählt ist, erfolgt die Bereinigung des Archivs mit Hilfe der Konsolidierung (S. 492), was eine zeit- und ressourcenintensivere Aktion ist.

4.2.6.2 Schema Großvater-Vater-Sohn

Auf einen Blick

- Tägliche ('Sohn'), wöchentliche ('Vater') und monatliche ('Großvater') Backups
- Benutzerdefinierbarer Tag für wöchentliche und monatliche Backups
- Benutzerdefinierbare Aufbewahrungsdauer für Backups jeden Typs

Beschreibung

Angenommen, Sie wollen einen Backup-Plan aufstellen, der regelmäßig eine Serie täglicher (T), wöchentlicher (W) und monatlicher (M) Backups produziert. Beispiel: Die nachfolgende Tabelle zeigt eine exemplarische zweimonatige Periode für einen solchen Plan.

	Mo	Di	Mi	Do	Fr	Sa	So
Jan 1—Jan 7	T	T	T	T	W	-	-
Jan 8—Jan 14	T	T	T	T	W	-	-
Jan 15—Jan 21	T	T	T	T	W	-	-
Jan 22—Jan 28	T	T	T	T	M	-	-
Jan 29—Feb 4	T	T	T	T	W	-	-
Feb 5—Feb 11	T	T	T	T	W	-	-
Feb 12—Feb 18	T	T	T	T	W	-	-
Feb 19—Feb 25	T	T	T	T	M	-	-
Feb 26—Mrz 4	T	T	T	T	W	-	-

Die täglichen Backups laufen an jedem Wochentag außer freitags, welcher für wöchentliche und monatliche Backups gelassen wird. Die monatlichen Backups laufen am letzten Freitag eines jeden Monats, während die wöchentlichen Backups an allen übrigen Freitagen laufen. Als Ergebnis erhalten Sie normalerweise 12 monatliche Backups über ein vollständiges Jahr hinweg.

Parameter

Sie können für ein Schema Großvater-Vater-Sohn (GVS) folgende Parameter einstellen.

Backup starten	Spezifiziert, wann das Backup starten soll. Der Standardwert ist 12:00 Uhr.
Backup auf	Spezifizieren Sie die Tage in der Woche, an denen ein Backup ausgeführt wird. Der Standardwert ist **Werktags**.
Wöchentlich/monatlich:	Spezifiziert, welchen Tag in der Woche (der im Feld **Backup an** gewählten Tage) Sie für wöchentliche und monatliche Backups reservieren wollen. Der Standardwert ist **Freitag**. Mit diesem Wert wird ein monatliches Backup am letzten Freitag eines jeden Monats ausgeführt. Wöchentliche Backups werden an allen anderen Freitagen ausgeführt. Sollten Sie einen anderen Tag der Woche wählen, dann werden diese Regeln auf den ausgewählten Tag angewendet.
Backups behalten	Spezifiziert, wie lange die Backups im Archiv gespeichert werden sollen. Die Zeitdauer kann in Stunden, Tagen, Wochen, Monaten oder Jahren gesetzt werden. Für monatliche Backups können Sie auch **Unbegrenzt behalten** wählen, falls Sie diese für immer speichern wollen. Die Standardwerte für jeden Backup-Typ sind wie folgt: Täglich: 5 Tage (empfohlenes Minimum) Wöchentlich: 7 Wochen Monatlich: unbegrenzt Die Aufbewahrungsdauer für wöchentliche Backups muss die für tägliche überschreiten; die Periode für monatliche Backups muss größer sein als die für wöchentliche. Es wird für tägliche Backups eine Aufbewahrungsdauer von wenigstens einer Woche empfohlen.
Backup-Typ	Spezifiziert den Typ täglicher, wöchentlicher und monatlicher Backups ■ **Immer vollständig** – alle täglichen, wöchentlichen und monatlichen Backups sind immer vollständig. Das ist die Standardauswahl für Fälle, in denen ein Bandgerät als Backup-Speicherort ausgewählt wird. ■ **Vollständig/Differentiell/Inkrementell** – tägliche Backups sind inkrementell, wöchentliche Backups differentiell und monatliche Backups sind vollständig. Das erste Backup ist immer vollständig. Dies bedeutet jedoch nicht, dass es ein monatliches Backup ist. Es wird als tägliches, wöchentliches oder monatliches Backup aufbewahrt, abhängig vom Wochentag, an dem es erstellt wurde.
Erweiterte Einstellungen	Verfügbar nur für die Advanced Editionen von Acronis Backup & Recovery 11.5 und bei Erstellung eines zentralen Backup-Plans. Details finden Sie im Abschnitt 'Erweiterte Planungseinstellungen (S. 98)'.

Ein Backup wird solange nicht gelöscht, bis alle auf ihm beruhenden Backups ebenfalls von einer Löschung betroffen sind. Aus diesem Grund kann es sein, dass Sie ein Backup sehen (mit dem Symbol gekennzeichnet), welches noch einige Tage über sein Ablaufdatum im Archiv verbleibt.

Beispiele

Jeder Tag der vergangenen Woche, jede Woche des vergangenen Monats

Betrachten wir ein allgemein als nützlich angesehenes GVS-Backup-Schema.

- Dateien jeden Tag sichern, einschließlich am Wochenende
- Ermöglicht die Wiederherstellung von Dateien von jedem der vergangenen sieben Tage
- Zugriff auf die wöchentlichen Backups des vergangenen Monats haben.
- Monatliche Backups unbegrenzt behalten.

Die Parameter des Backup-Schemas können dann wie folgt gesetzt werden.

- Backup starten: **23:00:00 Uhr**
- Sichern: **Alle Tage**
- Wöchentlich/monatlich: **Samstag** (als Beispiel)
- Backups aufbewahren:
  - Täglich: **1 Woche**
  - Wöchentlich: **1 Monat**
  - Monatlich: **unbegrenzt**

Als Ergebnis wird ein Archiv aus täglichen, wöchentlichen und monatlichen Backups erstellt. Tägliche Backups sind für die sieben Tage seit Erstellung verfügbar. Ein Beispiel: Ein tägliches Backup vom Sonntag (1. Januar) wird bis zum nächsten Sonntag (8. Januar) verfügbar sein, das erste wöchentliche Backup vom Samstag (7. Januar) wird auf dem System bis zum 7. Februar gespeichert. Monatliche Backups werden nie gelöscht.

Begrenzte Speicherung

Sofern Sie nicht eine Unmenge von Platz zur Speicherung eines riesigen Archivs einrichten wollen, sollten Sie ein GVS-Schema aufsetzen, welches Ihre Backups kurzlebiger macht, gleichzeitig aber auch sicherstellt, dass Ihre Informationen im Fall eines unbeabsichtigten Datenverlustes wiederhergestellt werden können.

Angenommen, Sie müssen:

- Backups am Ende eines jeden Arbeitstages durchführen
- fähig sein, eine versehentlich gelöschte oder ungewollt modifizierte Datei wiederherzustellen, falls dies relativ schnell entdeckt wurde
- zehn Tage nach seiner Erstellung noch Zugriff auf ein wöchentliches Backup haben
- monatliche Backups für ein halbes Jahr aufbewahren.

Die Parameter des Backup-Schemas können dann wie folgt gesetzt werden.

- Backup starten: **18:00:00 Uhr**
- Sichern: **Werktags**
- Wöchentlich/monatlich: **Freitag**
- Backups aufbewahren:
  - Täglich: **1 Woche**
  - Wöchentlich: **10 Tage**
  - Monatlich: **6 Monate**

Mit Hilfe dieses Schemas steht Ihnen eine Woche zur Verfügung, um die frühere Version einer beschädigten Datei aus einem täglichen Backup wiederherzustellen, außerdem haben Sie einen 10-Tage-Zugriff auf wöchentliche Backups. Jedes monatliche Voll-Backup wird über sechs Monate nach seinem Erstelldatum verfügbar sein.

Arbeitsplan

Angenommen, Sie sind Finanzberater in Teilzeit und arbeiten dienstags und donnerstags in einer Firma. An diesen Tagen führen Sie häufig Änderungen an Ihren Finanzdokumenten, Mitteilungen durch und aktualisieren Ihre Tabellenkalkulationen etc. auf Ihrem Notebook. Um diese Daten per Backup zu sichern, wollen Sie vermutlich:

- die Veränderungen an den finanziellen Mitteilungen, Tabellenkalkulationen etc. verfolgen, die Sie dienstags und donnerstags durchgeführt haben (tägliches inkrementelles Backup).
- eine wöchtenliche Zusammenfassung aller Dateiveränderungen seit dem letzten Monat haben (wöchentliche differentielle Backups am Freitag)
- ein monatliches Voll-Backup Ihrer Dateien haben.

Weiterhin sei angenommen, dass Sie sich einen Zugriff auf alle Backups, inkl. der täglichen, für wenigstens sechs Monate bewahren wollen.

Das nachfolgende GVS-Schema passt für diesen Zweck:

- Backup starten: **23:30 Uhr**
- Sichern: **Dienstag, Donnerstag, Freitag**
- Wöchentlich/monatlich: **Freitag**
- Backups aufbewahren:
  - Täglich: **6 Monate**
  - Wöchentlich: **6 Monate**
  - Monatlich: **5 Jahre**

Tägliche inkrementelle Backups werden hier dienstags und donnerstags erstellt, zusammen mit an Freitagen durchgeführten wöchentlichen und monatlichen Backups. Beachten Sie, dass um **Freitag** im Feld **Wöchentlich/monatlich** auswählen zu können, Sie ihn zuerst im Feld **Backup an** auswählen müssen.

Ein solches Archiv würde es Ihnen erlauben, Ihre Finanzdokumente vom ersten und letzten Tag der Arbeit zu vergleichen und eine fünfjährige Geschichte aller Dokumente zu haben.

Keine täglichen Backups

Betrachten Sie ein exotischeres GVS-Schema:

- Backup starten: **12:00 Uhr**
- Sichern: **Freitag**
- Wöchentlich/monatlich: **Freitag**
- Backups aufbewahren:
  - Täglich: **1 Woche**
  - Wöchentlich: **1 Monat**
  - Monatlich: **unbegrenzt**

Ein Backup wird daher nur freitags durchgeführt. Dies macht Freitag zur einzigen Wahl für wöchentliche und monatliche Backups, ohne dass ein Tag für tägliche Backups bleibt. Das

resultierende „Großvater-Vater“-Archiv wird daher nur aus wöchentlichen differentiellen und monatlichen vollständigen Backups bestehen.

Obwohl es möglich ist, GVS für die Erstellung eines solchen Archivs zu verwenden, ist das eigene Schema in dieser Situation flexibler.

4.2.6.3 Benutzerdefiniertes Backup-Schema

Auf einen Blick

- benutzerdefinierte Planung und Bedingungen für Backups jeden Typs
- Benutzerdefinierte Planungen und Aufbewahrungsregeln

Parameter

Parameter	Bedeutung
Planung für vollständige Backups	Spezifiziert, nach welcher Zeitplanung und unter welchen Bedingungen ein Voll-Backup durchgeführt werden soll. Ein Beispiel: Das Voll-Backup kann zur Ausführung an jedem Sonntag um 1:00 Uhr angesetzt werden, sobald alle Benutzer abgemeldet wurden.
Planung für inkrementelle Backups	Spezifiziert, nach welcher Zeitplanung und unter welchen Bedingungen ein inkrementelles Backup durchgeführt werden soll. Anstelle des inkrementellen wird ein Voll-Backup erstellt, sofern das Archiv zum Zeitpunkt der Task-Ausführung kein Voll-Backup enthält.
Planung für differentielle Backups	Spezifiziert, nach welcher Zeitplanung und unter welchen Bedingungen ein differentielles Backup durchgeführt werden soll. Anstelle des differentiellen wird ein Voll-Backup erstellt, sofern das Archiv zum Zeitpunkt der Task-Ausführung keine Voll-Backups enthält.
Archiv bereinigen	Gibt an, wie alte Backups entfernt werden sollen: entweder durch das regelmäßige Anwenden von Aufbewahrungsregeln (S. 108) oder durch das Bereinigen des Archivs während eines Backups, wenn am Zielspeicherort kein Platz mehr verfügbar ist. Standardmäßig sind keine Aufbewahrungsregeln angegeben und alte Backups daher nicht automatisch gelöscht. **Aufbewahrungsregeln verwenden** Spezifizieren Sie die Aufbewahrungsregeln und wann diese angewendet werden sollen. Diese Einstellung empfiehlt sich für Backup-Ziele wie z.B. freigegebene Ordner oder zentrale Depots. **Wenn nicht ausreichend Speicherplatz während des Backups vorhanden ist** Das Archiv wird nur während eines Backups bereinigt, sofern nicht ausreichend Speicherplatz für ein neues Backup vorhanden ist. In diesem Fall verhält sich die Software folgendermaßen: ▪ Das älteste Voll-Backup einschließlich aller abhängigen inkrementellen bzw. differentiellen Backups wird gelöscht ▪ Wenn nur ein vollständiges Backup vorhanden ist und ein neues Voll-Backup gerade erstellt wird, dann wird das letzte vollständige Backup mit allen abhängigen inkrementellen bzw. differentiellen Backups gelöscht. ▪ Wenn nur ein vollständiges Backup vorhanden ist und ein inkrementelles

	bzw. differentielles Backup gerade erstellt wird, erscheint eine Fehlermeldung, dass nicht genügend freier Speicher vorhanden ist. Diese Einstellung empfiehlt sich bei der Sicherung auf einem USB-Laufwerk oder der Acronis Secure Zone. Die Einstellung ist nicht auf verwaltete Depots sowie FTP- und SFTP-Server anwendbar. Mit dieser Einstellung kann das letzte Backup im Archiv gelöscht werden, falls auf dem Speichermedium nicht ausreichend Platz für mehr als ein Backup vorhanden ist. Bedenken Sie jedoch, dass Ihnen damit möglicherweise kein Backup bleibt, falls das Programm aus irgendeinem Grund das neue Backup nicht erstellen kann.
Aufbewahrungsregeln anwenden (nur wenn Aufbewahrungsregeln erstellt wurden)	Spezifiziert, wann die Aufbewahrungsregeln (S. 108) angewendet werden. Die Bereinigungsprozedur kann z.B. so aufgesetzt werden, dass sie nach jedem Backup und zudem nach Zeitplanung abläuft. Diese Option ist nur dann verfügbar, wenn Sie wenigstens eine Regel in den **Aufbewahrungsregeln** definiert haben.
Planung für Bereinigung (nur wenn **Nach Planung** ausgewählt ist)	Spezifiziert einen Zeitplan zur Bereinigung des Archivs. Die Bereinigung kann z.B. so definiert werden, dass sie planmäßig am letzten Tag eines jeden Monats startet. Diese Option ist nur verfügbar, wenn Sie **Nach Planung** unter **Aufbewahrungsregeln anwenden** gewählt haben.
2. Speicherort, **3. Speicherort**, usw.	Spezifiziert, wohin die Backups vom aktuellen Speicherort aus kopiert oder verschoben (S. 104) werden sollen. Diese Option ist nur verfügbar, wenn Sie entweder das Kontrollkästchen **Neu erstelltes Backup zu einem anderen Speicherort replizieren** unter **Art des Backups** aktiviert haben – oder das Kontrollkästchen **Die ältesten Backups an einen anderen Speicherort verschieben** im Fenster **Aufbewahrungsregeln**.

Beispiele

Wöchentliches Voll-Backup

Das folgende Schema bringt ein Voll-Backup hervor, das jede Freitagnacht erstellt wird.

Voll-Backup: **Planung: Wöchentlich** jeden **Freitag** um **22:00 Uhr**

Hier werden alle Parameter außer **Planung** bei **Voll-Backup** leer gelassen. Alle Backups in diesem Archiv werden unbegrenzt behalten (es wird keine Bereinigung des Archivs vorgenommen).

Voll- und inkrementelles Backup plus Bereinigung

Mit dem nachfolgenden Schema wird das Archiv aus wöchentlichen Voll-Backups und täglichen inkrementellen Backups bestehen. Eine zusätzliche Bedingung ist, dass ein Voll-Backup nur startet, wenn sich alle Benutzer abgemeldet haben.

Voll-Backup: Planung: Wöchentlich jeden **Freitag** um **22:00 Uhr**

Voll-Backup: Bedingungen: Benutzer ist abgemeldet

Inkrementell: Planung: Wöchentlich, an jedem Werktag um **21:00 Uhr**

Weiterhin sollen alle Backups, die älter als ein Jahr sind, aus dem Archiv gelöscht und die Bereinigung nach Erstellung eines neuen Backups durchgeführt werden.

Aufbewahrung: Lösche Backups älter als **12 Monate**

Aufbewahrungsregeln anwenden: Nach Backup

Vorgegeben ist, dass einjährige Backups solange nicht gelöscht werden, bis alle davon abhängenden inkrementellen Backups ebenfalls Objekt einer Löschaktion werden. Weitere Informationen finden Sie bei Aufbewahrungsregeln (S. 108).

Monatliche Voll-, wöchentliche differentielle und tägliche inkrementelle Backups plus Bereinigung

Dieses Beispiel demonstriert die Verwendung aller im benutzerdefinierten Schema verfügbaren Optionen.

Angenommen, Sie benötigen ein Schema, das monatliche Voll-Backups, wöchentliche differentielle und tägliche inkrementelle Backups produziert. Die Backup-Planung sieht dann wie folgt aus.

Voll-Backup: Planung: Monatlich jeden **letzten Sonntag** des Monats um **21:00 Uhr**

Inkrementell: Planung: Wöchentlich jeden **Werktag** um **19:00 Uhr**

Differentiell: Planung: Wöchentlich jeden **Samstag** um **20:00 Uhr**

Weiterhin wollen Sie Bedingungen hinzufügen, die erfüllt sein müssen, damit ein Backup-Task startet. Diese werden im Feld **Bedingungen** für jeden Backup-Typ eingestellt.

Voll-Backup: **Bedingungen**: **Speicherort verfügbar**

Inkrementell: **Bedingungen**: **Benutzer ist abgemeldet**

Differentiell: **Bedingungen**: **Benutzer ist untätig**

Als Folge startet ein Voll-Backup – ursprünglich für 21:00 geplant – möglicherweise später: sobald der Backup-Speicherort verfügbar wird. Vergleichbar warten die Backup-Tasks für inkrementelle bzw. differentielle Backups solange, bis alle Benutzer abgemeldet bzw. untätig sind.

Abschließend erstellen Sie Aufbewahrungsregeln für das Archiv: Behalten Sie nur Backups, die nicht älter als sechs Monate sind, und lassen Sie die Bereinigung nach jedem Backup-Task sowie an jedem letzten Tag eines Monats ausführen.

Aufbewahrungsregeln: Lösche Backups älter als **6 Monate**

Aufbewahrungsregeln anwenden: **Nachdem Backup**, **nach Planung**

Planung für die Bereinigung: **Monatlich** am **letzten Tag** von **allen Monaten** um **22:00 Uhr**

Standardmäßig wird ein Backup solange nicht gelöscht, wie es abhängige Backups hat, die behalten werden müssen. Wird z.B. ein Voll-Backup einer Löschaktion unterworfen, während es noch inkrementelle oder differentielle, von ihm abhängende Backups gibt, so wird die Löschung solange verschoben, bis alle abhängenden Backups ebenfalls gelöscht werden können.

Weitere Informationen finden Sie bei Aufbewahrungsregeln (S. 108).

4.2.6.4 Schema 'Türme von Hanoi'

Auf einen Blick

- bis zu 16 Level mit vollständigen, differentiellen und inkrementellen Backups

- Backups des nächsten Levels sind doppelt so selten wie die des vorherigen Levels
- Es wird jeweils ein Backup eines Levels gespeichert.
- eine höhere Dichte hin zu jüngeren Backups

Parameter

Sie können beim Schema Türme von Hanoi die folgenden Parameter einstellen.

Planung	Einen tдglichen (S. 90), wцchentlichen (S. 92) oder monatlichen (S. 94) Zeitplan einstellen. Bei der Konfiguration von Planungseinstellungen haben Sie auch die Möglichkeit, einfache Planungen zu erstellen (beispielsweise eine einfache tägliche Planung: ein Backup-Task wird täglich um 10 Uhr ausgeführt) – genauso wie auch komplexere Zeitpläne (Beispiel für einen komplexen täglichen Plan: ein Task wird jeden dritten Tag ausgeführt, beginnend vom 15. Januar. An den betreffenden Tagen wird der Task alle 2 Stunden von 10:00 bis 22:00 Uhr wiederholt). Auf diese Weise spezifizieren komplexe Zeitpläne die Sitzungen, an denen das Schema ausgeführt werden soll. In der nachfolgenden Betrachtung können „Tage“ durch „geplante Sitzungen“ ersetzt werden.
Zahl der Level	Bestimmen Sie zwischen 2 bis 16 Backup-Level. Zu Details siehe die nachfolgend dargestellten Beispiele.
Roll-Back-Zeitspanne	Garantierte Zahl von Sitzungen, die Sie jederzeit im Archiv zurückgehen können. Automatisch kalkuliert, abhängig von den Zeitplan-Parametern und der gewählten Level-Zahl. Zu Details siehe das nachfolgend dargestellte Beispiel.
Backup-Typ	Spezifiziert, welche Backup-Typen die Backup-Level haben werden ▪ **Immer vollständig** – alle Level der Backups werden vom Typ 'Vollständig' sein. Das ist die Standardauswahl für Fälle, in denen ein Bandgerät als Backup-Speicherort ausgewählt wird. ▪ **Vollständig/Differentiell/Inkrementell** – die Backups verschiedener Level werden verschiedene Typen haben: – Backups des letzten Levels sind vollständig – Backups zwischenzeitlicher Level sind differentiell – Backups des ersten Levels sind inkrementell

Beispiel

Die **Zeitplan**-Parameter sind wie folgt eingestellt

- Wiederholen: Jeden Tag
- Frequenz: Einmalig um 18:00 Uhr

Zahl der Level: 4

Backup-Typ: Vollständig/Differentiell/Inkrementell

So sieht der Zeitplan der ersten 14 Tage (oder 14 Sitzungen) für dieses Schema aus. Schattierte Zahlen kennzeichnen die Backup-Level.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
4	1	2	1	3	1	2	1	4	1	2	1	3	1

Die Backups unterschiedlicher Level haben unterschiedliche Typen:

- *Letzte-Ebene*-Backups (hier Ebene 4) sind Voll-Backups;
- Die Backups *zwischenzeitlicher Ebenen* (2, 3) sind differentiell;

- *Erste-Ebene* -Backups (1) sind inkrementell.

Ein Bereinigungsmechanismus stellt sicher, dass nur die jeweils neusten Backups jeder Ebene behalten werden. So sieht das Archiv am 8. Tag aus, ein Tag vor Erstellung eines neuen Voll-Backups.

1	2	3	4	5	6	7	8
4	1	2	1	3	1	2	1

Das Schema erlaubt eine effiziente Datenspeicherung: mehr Backups sammeln sich zur gegenwärtigen Zeit hin an. Mit vier Backups können Sie die Daten von heute, gestern, vor einer halben oder einer ganzen Woche wiederherstellen.

Roll-Back-Zeitspanne

Die Zahl der Tage, die Sie im Archiv zurückgehen können, variiert in Abhängigkeit von den Tagen: Die garantiert verfügbare, minimale Zahl an Tagen wird Roll-Back Periode genannt.

Die nachfolgende Tabelle zeigt Voll-Backups und Roll-Back Perioden für Schemata mit unterschiedlichen Leveln.

Zahl der Level	Voll-Backup alle	Zurück an unterschiedlichen Tagen	Roll-Back-Zeitspanne
2	2 Tage	1 bis 2 Tage	1 Tag
3	4 Tage	2 bis 5 Tage	2 Tage
4	8 Tage	4 bis 11 Tage	4 Tage
5	16 Tage	8 bis 23 Tage	8 Tage
6	32 Tage	16 bis 47 Tage	16 Tage

Durch Hinzufügen eines Levels werden Voll-Backup und Roll-back-Perioden jeweils verdoppelt.

Warum die Zahl von Wiederherstellungstagen variiert, ergibt sich aus dem vorherigen Beispiel.

Das sind die verfügbaren Backups am 12. Tag (Zahlen in Grau kennzeichnen gelöschte Backups).

1	2	3	4	5	6	7	8	9	10	11	12
4	1	2	1	3	1	2	1	4	1	2	1

Das Backup vom 5. Tag liegt immer noch vor, weil bisher kein neues differentielles Backup für Level 3 erstellt wurde. Da es auf dem Voll-Backup von Tag 1 basiert, ist dieses Backup ebenfalls verfügbar. Dies ermöglicht es, bis zu 11 Tage zurückzugehen, was dem Best-Case-Szenario entspricht.

Am folgenden Tag wird jedoch ein neues differentielles Backup der dritten Ebene erstellt und das alte Voll-Backup gelöscht.

1	2	3	4	5	6	7	8	9	10	11	12	13
4	1	2	1	3	1	2	1	4	1	2	1	3

Dies ermöglicht nur ein Wiederherstellungs-Intervall von 4 Tagen, was dem Worst-Case-Szenario entspricht.

Am Tag 14 beträgt das Intervall 5 Tage. Es steigt an den nachfolgenden Tagen, bevor es wieder abnimmt – und so weiter.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
4	1	2	1	3	1	2	1	4	1	2	1	3	1

Die Roll-Back-Periode verdeutlicht, wie viele Tage auch im schlimmsten Fall garantiert verfügbar sind. Bei einem Vier-Level-Schema beträgt sie vier Tage.

4.2.6.5 Manueller Start

Mit dem Schema **Manueller Start** müssen Sie keine Backup-Planung spezifizieren. Sie können den Backup-Plan von der Ansicht **Pläne und Tasks** jederzeit später manuell ausführen.

Spezifizieren Sie die passenden Einstellungen wie folgt.

Backup-Typ

Wählen Sie den Typ des Backups

- **Vollständig.** Standardmäßig für alle Backup-Speicherorte (mit Ausnahme des Acronis Online Backup Storages) vorausgewählt.
- **Inkrementell.** Beim ersten Mal wird ein Voll-Backup erstellt. Die nachfolgenden Backups werden inkrementell. Als einziger Backup-Typ für den Acronis Online Backup Storage ausgewählt.
- **Differentiell.** Beim ersten Mal wird ein Voll-Backup erstellt. Die nächsten Backups werden differentiell.

4.2.6.6 Initial Seeding

Dieses Backup-Schema ist verfügbar, wenn der Acronis Online Backup Storage als Backup-Ziel ausgewählt wurde. Ein Backup ist nur dann erfolgreich, wenn Sie eine Initial Seeding-Lizenz haben.

Der 'Initial Seeding'-Dienst ist in Ihrer Region möglicherweise nicht verfügbar. Klicken Sie hier für weitere Informationen: http://kb.acronis.com/content/15118.

Initial Seeding ermöglicht Ihnen, das erste Backup (üblicherweise ein Voll-Backup und sehr groß) durch Verwendung einer Festplatte (oder ähnlichen Laufwerks) statt per Internetübertragung zum Online Storage hochzuladen. Nachfolgende Backups (üblicherweise inkrementell und daher deutlich kleiner) können dann per Internet übertragen werden, sobald das Voll-Backup im Online Storage angekommen ist.

Wenn Sie eine Datenmenge von 100 GB oder mehr sichern, ermöglicht Initial Seeding eine schnellere Auslieferung der Daten und geringere Übertragungskosten.

Konsultieren Sie zu weiteren Details den Abschnitt „Initial Seeding FAQ (S. 465)“.

4.2.7 Archiv-Validierung

Setzen Sie einen Validierungstask auf, um zu überprüfen, ob gesicherte Daten wiederherstellbar sind. Der Validierungstask scheitert und der Backup-Plan erhält den Status **Error**, wenn das Backup die Überprüfung nicht erfolgreich bestehen konnte.

Die Validierung eines Datei-Backups imitiert die Wiederherstellung aller Dateien aus einem Backup an einen imitierten Zielort. Die Validierung eines Image-Backups berechnet eine Prüfsumme für jeden Datenblock, der im Backup gespeichert ist.

Spezifizieren Sie die folgenden Parameter, um eine Validierung anzulegen

1. **Validierungszeitpunkt** – bestimmen Sie, wann die Validierung durchgeführt wird. Da eine Validierung eine Ressourcen-intensive Aktion ist, empfiehlt es sich, sie so zu **planen**, dass sie nicht zu Hauptbelastungszeiten der verwalteten Maschine erfolgt. Wenn die Validierung dagegen

ein wichtiger Teil Ihrer Strategie zur Datensicherung ist und Sie es bevorzugen, sofort informiert zu werden, ob die gesicherten Daten intakt und daher erfolgreich wiederherstellbar sind, dann sollten Sie die Validierung direkt nach Backup-Erstellung durchführen.

2. **Was validieren** – bestimmen Sie, ob das komplette Archiv oder das letzte Backup im Archiv überprüft wird.

   Die Validierung eines Archivs überprüft alle Backups des Archivs und kann viel Zeit sowie System-Ressourcen benötigen.

   Die Validierung des letzten Backups kann auch Zeit benötigen, selbst wenn dieses Backup inkrementell oder differentielle ist und nur eine geringe Größe hat. Hintergrund ist, dass die Aktion nicht einfach nur die konkret im Backup enthaltenen Daten validiert, sondern alle durch Wahl des Backups wiederherstellbaren Daten. Dies erfordert einen Zugriff auf zuvor erstellte Backups.

3. **Validierungsplanung** (erscheint nur, falls Sie in Schritt 1 **Nach Zeitplan** ausgewählt haben) – definiert den Zeitplan für die Validierung. Zu weiteren Informationen siehe den Abschnitt Planung (S. 89).

4.2.8 Anmeldedaten des Backup-Plans

Stellen Sie die Anmeldedaten für das Konto zur Verfügung, unter dem der Plan ausgeführt wird.

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Anmeldedaten des Acronis Service verwenden** oder **Unter dem aktuellen Benutzer ausführen**

     Der Plan wird unter einem der folgenden Benutzerkonten ausgeführt:
     - Das Konto des Agenten-Dienstes (Agent Service), sofern Sie administrative Berechtigungen auf der Maschine haben.
     - Ihr Konto, sofern Sie als normaler Benutzer angemeldet sind (etwa als Mitglied der Gruppe 'Benutzer').
   - **Folgende Anmeldedaten verwenden**

     Die Tasks werden immer mit den von Ihnen spezifizierten Anmeldedaten ausgeführt, egal ob manuell oder per Zeit-/Ereignis-Planung gestartet.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
     - **Kennwort bestätigen**. Geben Sie das Kennwort erneut ein.
2. Klicken Sie auf **OK**.

Siehe den Abschnitt Benutzerberechtigungen auf einer verwalteten Maschine (S. 37), um mehr über Aktionen zu erfahren, die in Abhängigkeit von Benutzerberechtigungen verfügbar sind.

4.2.9 Bezeichnung (Maschinen-Eigenschaften in einem Backup bewahren)

Jedes Mal, wenn eine Maschine gesichert wird, werden dem Backup auch Informationen über den Maschinennamen, das Betriebssystem, das Windows Service Pack sowie den 'Security Identifier' (SID)

hinzugefügt – ergänzt um eine benutzerdefinierte Textbezeichnungen. Die Bezeichnung kann Angaben zur Abteilung, zum Namen des Maschinen-Benutzers oder ähnliche Informationen enthalten, die als Kennzeichnung (Tag) oder Suchschlüssel dienen können.

Wenn Sie die Maschine mit dem Agenten für ESX(i) zu einem VMware ESX(i)-Server wiederherstellen (S. 146) oder das Backup zu einer virtuellen ESX(i)-Maschine konvertieren (S. 192), dann werden diese Eigenschaften in die Konfiguration der virtuellen Maschine übertragen. Sie können diese dann in den Einstellungen der virtuellen Maschine einsehen: **Einstellungen bearbeiten** –> **Optionen** –> **Erweitert** –> **Allgemein** –> **Konfigurationsparameter**. Sie können die virtuellen Maschinen mit Hilfe dieser einstellbaren Parameter sortieren oder gruppieren. Das kann bei verschiedenen Szenarien nützlich sein.

Beispiel:

Angenommen, Sie möchten Ihr Büro oder Datacenter in eine virtuelle Umgebung migrieren. Sie können durch die Verwendung von Dritthersteller-Software, die per VMware-API auf die Konfigurationsparameter zugreifen kann, Sicherheitsrichtlinien auf jede Maschine anwenden – sogar bevor diese eingeschaltet wird.

So fügen Sie Backups eine Textbezeichnung hinzu:

1. Klicken Sie auf der Seite **Backup-Plan erstellen** (S. 58) auf **Anmeldedaten des Plan, Kommentare, Bezeichnung anzeigen**.
2. Geben Sie im Feld **Bezeichnung** die gewünschte Benennung ein – oder wählen Sie eine aus dem aufklappbaren Menü aus.

Spezifikation der Parameter

Parameter	Wert	Beschreibung
acronisTag.label	<string>	Eine benutzerdefinierte Bezeichnung. Die Bezeichnung kann von einem Benutzer bei Erstellung eines Backup-Plans festgelegt werden.
acronisTag.hostname	<string>	Host-Name (FQDN)
acronisTag.os.type	<string>	Betriebssystem
acronisTag.os.servicepack	0, 1, 2...	Die Version des im System installierten Service Packs. Nur für Windows-Betriebssysteme.
acronisTag.os.sid	<string>	Die SID der Maschine. Beispielsweise: S-1-5-21-874133492-782267321-3928949834. Nur für Windows-Betriebssysteme.

Werte des Parameters 'acronisTag.os.type'

Windows NT 4	winNTGuest
Windows 2000 Professional	win2000ProGuest
Windows 2000 Server	win2000ServGuest
Windows 2000 Advanced Server	win2000ServGuest
Windows XP – alle Editionen	winXPProGuest
Windows XP – All Editionen (64 Bit)	winXPPro64Guest
Windows Server 2003 – alle Editionen	winNetStandardGuest
Windows Server 2003 – All Editionen (64 Bit)	winNetStandard64Guest

Windows 2008	winLonghornGuest
Windows 2008 (64 Bit)	winLonghorn64Guest
Windows Vista	winVistaGuest
Windows Vista (64 Bit)	winVista64Guest
Windows 7	windows7Guest
Windows 7 (64 Bit)	windows7_64Guest
Windows Server 2008 R2 (64 Bit)	windows7Server64Guest
Linux	otherLinuxGuest
Linux (64 Bit)	otherLinux64Guest
Anderes Betriebssystem	otherGuest
Anderes Betriebssystem (64 Bit)	otherGuest64

Beispiel

acronisTag.label = "DEPT:BUCH; COMP:SUPERSERVER; OWNER:EJONSON"

acronisTag.hostname = "superserver.corp.local"

acronisTag.os.type = "windows7Server64Guest"

acronisTag.os.servicepack = "1"

acronisTag.os.sid = "S-1-5-21-874133492-782267321-3928949834"

4.2.10 Die Reihenfolge von Aktionen in einem Backup-Plan

Falls ein Backup-Plan mehrere Aktionen enthält, führt Acronis Backup & Recovery 11.5 diese in folgender Reihenfolge aus:

1. Bereinigung (falls **Vor dem Backup** konfiguriert) und Validierung (falls die Bereinigung ausgeführt wurde und die Validierung zur Ausführung **Nach Anwendung der Aufbewahrungsregeln** konfiguriert ist).

   Falls ein Backup während der Bereinigung zu einem anderen Speicherort verschoben wurde, werden alle Aktionen, die für die nachfolgenden Speicherort konfiguriert wurden, zuerst durchgeführt, bevor mit den nachfolgenden Schritten für den primären Speicherort fortgefahren wird.
2. Befehlsausführung vor dem Backup.
3. Backup:
   a. Befehlsausführung vor Datenerfassung
   b. Snapshot-Erstellung
   c. Befehlsausführung nach Datenerfassung
   d. Backup-Prozess
4. Start der Backup-Katalogisierung

   Die Backup-Katalogisierung kann ein zeitaufwendiges Verfahren sein. Sie wird parallel mit den nachfolgenden Schritten ausgeführt.
5. Befehlsausführung nach dem Backup.
6. Desaster-Recovery-Plan (DRP)-Erstellung.
7. Konvertierung zu einer virtuellen Maschine.
8. Backup-Replikation.
9. Bereinigung.

Falls die Replikation stattgefunden hat oder ein Backup während der Bereinigung zu einem anderen Speicherort verschoben wurde, werden alle Aktionen, die für die nachfolgenden Speicherort konfiguriert wurden, zuerst durchgeführt, bevor mit den nachfolgenden Schritten für den primären Speicherort fortgefahren wird.

10. Validierung.
11. Bandauswurf.
12. Versenden von E-Mail-Benachrichtigung.

4.2.11 Warum fragt das Programm nach einem Kennwort?

Ein geplanter oder aufgeschobener Task muss unabhängig davon, ob ein Benutzer angemeldet ist, ausgeführt werden. In Fällen, in denen Sie die Anmeldedaten, unter denen ein Task ausgeführt wird, nicht explizit angegeben haben, schlägt das Programm die Verwendung Ihres Benutzerkontos vor. Geben Sie Ihr Kennwort ein, spezifizieren Sie ein anderes Konto oder ändern Sie die geplante Ausführung auf manuell.

4.3 Vereinfachte Benennung von Backup-Dateien

Gehen Sie folgendermaßen vor, um die vereinfachte Benennung von Backup-Dateien verwenden zu können:

- Klicken Sie in der Willkommensseite auf **Backup-Plan erstellen** (S. 58), erweitern Sie **Benennung der Backup-Datei, Archivkommentare anzeigen** und aktivieren Sie dann das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...**.

  Wenn Sie ein Backup von einem lokal angeschlossenen RDX- oder USB-Flash-Laufwerk erstellen, erscheint das Kontrollkästchen Backup-Dateien unter Verwendung des Archivnamens benennen... nicht. Stattdessen bestimmt der Wechsellaufwerksmodus (S. 221), ob das Standard- oder das vereinfachte Bennenungsschema verwendet wird. Unter Linux erscheint das Kontrollkästchen, nachdem Sie das Gerät manuell gemountet haben.

- Klicken Sie in der Willkommensseite auf **Backup jetzt** (S. 58). Die 'vereinfachte Benennung' wird immer dann verwendet, wenn das Backup-Ziel dies unterstützt (zu den Beschränkungen siehe weiter unten).

Wenn Sie die vereinfachte Dateibenennung verwenden, gilt:

- Der Dateiname des ersten (vollständigen) Backups im Archiv wird aus dem Archivnamen zusammengesetzt, beispielsweise: **MeineDateien.tib.** Die Dateinamen der nachfolgenden (inkrementellen oder differentiellen) Backups erhalten eine zusätzliche Kennziffer. Beispielsweise: **MeineDateien2.tib**, **MeineDateien3.tib** und so weiter.

  Diese einfache Namensschema ermöglicht Ihnen, von einer Maschine ein 'transportierbares' Image auf ein entfernbares Medium zu erstellen – oder die Backups durch Verwendung eines Skripts an einen anderen Speicherort zu verschieben.

- Die Software löscht vor Erstellung eines neuen Voll-Backups das komplette Archiv und startet danach ein neues.
- Dieses Verhalten ist nützlich, wenn Sie mehrere USB-Festplatten abwechselnd verwenden und jedes Laufwerk ein einzelnes Voll-Backup (S. 86) oder alle wдhrend einer Woche erstellten Backups (S. 87) behalten soll. Sie könnten am Ende aber ganz ohne Backups dastehen, falls ein Voll-Backup zu Ihrem einzigen Laufwerk fehlschlägt.
- Dieses Verhalten lässt sich aber unterdrücken, wenn Sie dem Archivnamen die [Datum]-Variable (S. 84) hinzufügen.

Wenn Sie die Standard-Dateibenennung verwenden, gilt:

- Jedes Backup erhält einen eindeutigen Dateinamen mit exaktem Datumsstempel und Backup-Typ. Beispielsweise: **MeineDateien_2010_03_26_17_01_38_960D.tib**. Diese Standard-Dateibenennung ermöglicht eine weitreichendere Nutzung von Backup-Zielorten und Backup-Schemata.

Einschränkungen

Bei Verwendung der vereinfachten Dateibenennung ist folgende Funktionalität nicht verfügbar:

- Konfiguration vollständiger, inkrementeller und differentieller Backups innerhalb eines einzigen Backup-Plans. Sie müssen separate Backup-Pläne für jeden Backup-Typ erstellen.
- Backups zu einem verwalteten Depot, auf Band, zu einer Acronis Secure Zone oder dem Acronis Online Backup Storage.
- Backups von virtuellen Maschinen mit dem Agenten für ESX(i) oder dem Agenten für Hyper-V.
- Replikation von Backups einrichten.
- Aufbewahrungsregeln konfigurieren.
- Regelmäßige Konvertierung von Backups zu einer virtuellen Maschine einrichten.
- Konvertierung eines inkrementellen oder differentiellen Backups zu einem Voll-Backup.

Beschränkungen bei Archivnamen

- Ein Archivname darf nicht mit einer Zahl enden.
- Folgende Zeichen sind bei FAT16-, FAT32- und NTFS-Dateisystemen für Dateinamen nicht erlaubt: Backslash (\), Schrägstrich (/), Doppelpunkt (:), Sternchen (Asterisk) (*), Fragezeichen (?), Anführungszeichen ("), Kleiner-als-Zeichen (<), Größer-als-Zeichen (>) und Hochstrich (|).

4.3.1 Die Variable '[DATE]'

Wenn Sie die Variable **[DATE]** zur Verwendung im Archivnamen spezifizieren, enthält der Dateiname eines jeden Backups sein entsprechendes Erstellungsdatum.

Bei Verwendung dieser Variable wird das erste Backup eines neuen Tages ein Voll-Backup. Die Software löscht vor Erstellung des nächsten Voll-Backups alle schon früher an diesem Tag erstellten Backups. Backups, die vor diesem Tag erstellt wurden, bleiben erhalten. Das bedeutet, dass Sie multiple Voll-Backups (mit oder ohne inkrementelle Erweiterungen) speichern können, jedoch nicht mehr als ein Voll-Backup pro Tag. Sie können die Backups nach Datum sortieren lassen. Sie können außerdem ein Skript verwenden, um ältere Backups zu kopieren, verschieben oder löschen.

Der Wert dieser Variablen ist das aktuelle Datum, eingefasst von Klammern ([]). Das Datumsformat hängt von den regionalen Einstellungen Ihrer Maschine ab. Falls das Datumsformat beispielsweise *Jahr-Monat-Tag* ist, dann ergibt der 31. Januar 2012 den Wert **[2012-01-31]**. Zeichen, die in Dateinamen nicht unterstützt werden (wie etwa Schrägzeichen (/)) werden durch Unterstriche (_) ersetzt.

Sie können die Variable an jeder Stelle im Archivnamen positionieren. Sie können zudem Groß- und Kleinbuchstaben in dieser Variable verwenden.

Beispiele

Beispiel 1: Angenommen Sie führen für zwei Tage, startend am 31.01.2012, zweimal täglich inkrementelle Backups aus (um Mitternacht und zur Mittagszeit). Der Archivname ist **MeinArchiv-[DATE]**, das Datumsformat ist *Jahr-Monat-Tag.* So sieht die Liste der Backup-Dateien nach dem zweiten Tag aus:

MeinArchiv-[2012-01-31].tib (vollständig, erstellt am 31. Januar um Mitternacht)
MeinArchiv-[2012-01-31]2.tib (inkrementell, erstellt am 31. Januar, zur Mittagszeit)
MeinArchiv-[2012-02-01].tib (vollständig, erstellt am 1. Februar um Mitternacht)
MeinArchiv-[2012-02-01]2.tib (inkrementell, erstellt am 1. Februar, zur Mittagszeit)

Beispiel 2: Angenommen, Sie erstellen Voll-Backups mit gleicher Planung, gleichem Archivnamen und Datumsformat wie im vorherigen Beispiel. In diesem Fall sieht die Liste der Backup-Dateien nach dem zweiten Tag wie folgt aus:

MeinArchiv-[2012-01-31].tib (vollständig, erstellt am 31. Januar, zur Mittagszeit)
MeinArchiv-[2012-02-01].tib (vollständig, erstellt am 1. Februar, zur Mittagszeit)

Hintergrund des Ergebnisses ist, dass die um Mitternacht erstellten Voll-Backups durch am selben Tag neu erstellte Voll-Backups ersetzt werden.

4.3.2 Backup-Aufteilung und vereinfachte Dateibenennung

Wenn ein Backup entsprechend der Einstellungen unter Backup-Aufteilung (S. 121) aufgesplittet wird, dann wird die gleiche Indizierung auch für die Namensteile des Backups verwendet. Der Dateiname für das nächste Backup erhält den nächsten verfügbaren Index.

Angenommen, das erste Backup des Archives **MeineDateien** wurde in zwei Teile aufgeteilt. Die Dateinamen dieses Backups sind folglich **MeineDateien1.tib** und **MeineDateien2.tib**. Das zweite Backup (als nicht aufgeteilt angenommen) wird **MeineDateien3.tib** genannt.

4.3.3 Verwendungsbeispiele

Dieser Abschnitt zeigt Ihnen Beispiele für die Verwendung der vereinfachten Dateibenennung.

4.3.3.1 Beispiel 1: Tägliches Backup ersetzt das alte

Betrachten Sie folgendes Szenario:

- Sie möchten Ihre Maschine mit einem täglichen Voll-Backup sichern.
- Sie wollen das Backup auf einer lokal angeschlossenen USB-Festplatte in der Datei **MeineMaschine.tib** speichern.
- Sie wollen, dass jedes neue Backup das jeweilige alte ersetzt.

Erstellen Sie in diesem Szenario einen Backup-Plan mit täglicher Planung. Spezifizieren Sie bei Erstellung des Backup-Plans die USB-Festplatte als Archiv-Speicherort und **MeineMaschine** als Archivnamen, aktivieren Sie dann das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...** und legen Sie danach **Voll** als Backup-Typ fest.

Ergebnis. Das Archiv besteht aus einer einzigen Datei: MeineMaschine.tib. Diese Datei wird vor Erstellung eines neuen Backups wieder gelöscht.

Falls Sie ein lokal angeschlossenes RDX-Laufwerk oder USB-Flash-Laufwerk zum Backup auswählen, wird Ihnen das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...** nicht angezeigt. Stellen Sie stattdessen sicher, dass der Wechsellaufwerksmodus (S. 221) auf **Wechselmedien** eingestellt ist.

4.3.3.2 Beispiel 2: Tägliche Voll-Backups mit Datumsstempel

Betrachten Sie folgendes Szenario:

- Sie möchten Ihre Maschine mit einem täglichen Voll-Backup sichern.
- Sie möchten ältere Backups per Skript zu einem Remote-Speicherort verschieben.

Erstellen Sie in diesem Szenario einen Backup-Plan mit täglicher Planung. Spezifizieren Sie bei Erstellung des Backup-Plans **MeineMaschine** als Archivnamen, aktivieren Sie dann das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...** und legen Sie danach **Voll** als Backup-Typ fest.

Ergebnis:

- Die Backups vom 1. Januar 2012, 2. Januar 2012 (usw.) werden entsprechend als 'MeineMaschine-[2012-01-01].tib', 'MeineMaschine-[2012-01-02].tib' (usw.) gespeichert.
- Ihr Skript kann ältere Backups auf Basis des Datumsstempels verschieben.

Siehe auch „Die Variable [Date]“ (S. 84).

4.3.3.3 Beispiel 3: Stündliche Backups innerhalb eines Tages

Betrachten Sie folgendes Szenario:

- Sie möchten von den wichtigsten Dateien Ihres Servers an jedem Tag stündliche Backups erstellen.
- Das erste Backup eines jeden Tages soll 'vollständig' sein und um Mitternacht ausgeführt werden – die nachfolgenden Backups des Tages sollen differentiell sein und um 01:00 Uhr, 02:00 Uhr (usw.) ausgeführt werden.
- Ältere Backups sollen im Archiv aufbewahrt werden.

Erstellen Sie in diesem Szenario einen Backup-Plan mit täglicher Planung. Spezifizieren Sie bei Erstellung des Backup-Plans **ServerDateien[Date]** als Archivnamen, aktivieren Sie das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...**, legen Sie **Differentiell** als Backup-Typ fest – und planen Sie dann für die Backups eine stündliche Ausführung (ab Mitternacht).

Ergebnis:

- Die 24 Backups vom 01.01.2012 werden als 'ServerDateien[2012-01-01].tib', 'ServerDateien[2012-01-01]2.tib' (usw.) bis zu 'ServerDateien[2012-01-01]24.tib' gespeichert.
- Die Backups des folgenden Tags starten mit einem Voll-Backup namens 'ServerDateien[2012-01-02].tib'.

Siehe auch „Die Variable [Date]“ (S. 84).

4.3.3.4 Beispiel 4. Tägliche Voll-Backups mit täglichem Laufwerkswechsel

Betrachten Sie folgendes Szenario:

- Sie möchten Ihre Maschine mit einem täglichen Voll-Backup sichern.
- Sie wollen das Backup auf einer lokal angeschlossenen USB-Festplatte in der Datei **MeineMaschine.tib** speichern.
- Sie haben zwei dieser Laufwerke. Sie möchten diese vor jedem Backup wechseln, so dass eines der Laufwerke die Backups von heute enthält, das andere die von gestern.

- Jedes neue Backup soll das Backup auf dem aktuell angeschlossenen Laufwerk ersetzen.

Erstellen Sie in diesem Szenario einen Backup-Plan mit täglicher Planung. Bei Erstellung des Backup-Plans:

- Spezifizieren Sie **MeineMachine** als Archivnamen.
- Spezifizieren Sie unter Windows **D:** als Archiv-Speicherort, wobei **D** der Laufwerksbuchstabe ist, den jedes der Laufwerke nach Anschluss an die Maschine im Betriebssystem hat.

  Erstellen Sie unter Linux ein Verzeichnis wie beispielsweise **/mnt/backup** und spezifizieren Sie es als Archiv-Speicherort. Stellen Sie sicher, dass Sie bei jedem Anschluss eines Laufwerks dieses an den Mount-Punkt **/mnt/backup** mounten.
- Aktivieren Sie das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...**.
- Wählen Sie **Vollständig** als Backup-Typ.

Ergebnis: Jedes Laufwerk wird nur je ein Voll-Backup enthalten. Während ein Laufwerk an die Maschine angeschlossen ist, können Sie das andere zur Erreichung einer zusätzlichen Datensicherheit außer Haus lagern.

Falls Sie unter Windows lokal angeschlossene RDX-Laufwerke oder USB-Flash-Laufwerke zum Backup auswählen, wird Ihnen das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...** nicht angezeigt. Stellen Sie stattdessen sicher, dass der Wechsellaufwerksmodus (S. 221) auf **Wechselmedien** eingestellt ist.

4.3.3.5 Beispiel 5. Tägliche Voll-Backups mit wöchentlichen Laufwerkswechsel

Betrachten Sie folgendes Szenario:

- Sie möchten Ihre Maschine mit täglichen Backups sichern: ein Voll-Backup an jedem Montag und inkrementelle Backups von Dienstag bis Sonntag.
- Sie wollen die Backups auf einer lokal angeschlossenen USB-Festplatte im Archiv **MeineMaschine.tib** speichern.
- Sie haben zwei dieser Laufwerke. Diese sollen an jedem Montag gewechselt werden, so dass ein Laufwerk die Backups der aktuellen Woche (Montag bis Sonntag) enhält – und das andere Laufwerk die Backups der letzten Woche.

Sie müssen in diesem Szenario zwei Backup-Pläne folgendermaßen erstellen:

a) Bei Erstellung des ersten Backup-Plans:

   - Spezifizieren Sie **MeineMachine** als Archivnamen.
   - Spezifizieren Sie unter Windows **D:** als Archiv-Speicherort, wobei **D** der Laufwerksbuchstabe ist, den jedes der Laufwerke nach Anschluss an die Maschine im Betriebssystem hat.

     Erstellen Sie unter Linux ein Verzeichnis wie beispielsweise **/mnt/backup** und spezifizieren Sie es als Archiv-Speicherort. Stellen Sie sicher, dass Sie bei jedem Anschluss eines Laufwerks dieses an den Mount-Punkt **/mnt/backup** mounten.
   - Aktivieren Sie das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...**.
   - Wählen Sie **Vollständig** als Backup-Typ.
   - Planen Sie die Backups so, dass Sie jede Woche am Montag laufen.

b) Spezifizieren Sie bei Erstellung des zweiten Backup-Plans dieselben Einstellungen wie im ersten Backup-Plan, nur dass Sie **Inkrementell** als Backup-Typ wählen und für die Backups eine wöchentliche Ausführung von Dienstag bis Sonntag planen.

Ergebnis:

- Bevor das 'Montags-Backup' erstellt wird (durch den ersten Backup-Plan), werden alle auf dem aktuell angeschlossenen Laufwerk liegenden Backups gelöscht.
- Während ein Laufwerk an die Maschine angeschlossen ist, können Sie das andere zur Erreichung einer zusätzlichen Datensicherheit außer Haus lagern.

Falls Sie unter Windows lokal angeschlossene RDX-Laufwerke oder USB-Flash-Laufwerke zum Backup auswählen, wird Ihnen das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...** nicht angezeigt. Stellen Sie stattdessen sicher, dass der Wechsellaufwerksmodus (S. 221) auf **Wechselmedien** eingestellt ist.

4.3.3.6 Beispiel 6: Backups während der Arbeitszeit

Betrachten Sie folgendes Szenario:

- Sie möchten von den wichtigsten Dateien Ihres Servers an jedem Tag Backups erstellen.
- Das erste Backup eines Tages soll vollständig sein und um 01:00 Uhr ausgeführt werden.
- Die Backups während der Arbeitszeit sollen differentiell sein und stündlich von 8:00 Uhr bis 17:00 Uhr ausgeführt werden.
- Dem Namen einer jeden Backup-Datei soll das Erstellungsdatum hinzugefügt werden.

Sie müssen in diesem Szenario zwei Backup-Pläne folgendermaßen erstellen:

a) Spezifizieren Sie bei Erstellung des ersten Backup-Plans **ServerDateien[DATE]** als Archivnamen, aktivieren Sie das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...**, legen Sie **Voll** als Backup-Typ fest – und planen Sie dann für die Backups eine tägliche Ausführung um 01:00 Uhr.

b) Spezifizieren Sie bei Erstellung des zweiten Backup-Plans dieselben Einstellungen wie im ersten Backup-Plan, nur dass Sie **Differentiell** als Backup-Typ wählen und die Backups folgendermaßen planen:

  - **Task starten**: **täglich**
  - **Alle**: **1 Stunde(n)**
  - **Von**: **08:00:00 Uhr**
  - **Bis**: **17:01:00 Uhr**

Ergebnis:

- Das Voll-Backup vom 31.01.2012 wird als 'ServerDateien[2012-01-31].tib' gespeichert.
- Die 10 differentiellen Backups vom 31.01.2012 werden als 'ServerDateien[2012-01-31]2.tib', 'ServerDateien[2012-01-31]3.tib' (usw.) bis zu 'ServerDateien[2012-01-31]11.tib' gespeichert.
- Die Backups des folgenden Tags (1. Februar) starten mit einem Voll-Backup namens 'ServerDateien[2012-02-01].tib'. Die differentiellen Backups starten mit 'ServerDateien[2012-02-01]2.tib'.

Siehe auch „Die Variable [Date]“ (S. 84).

4.4 Planung

Der Acronis-Scheduler hilft dem Administrator, Backup-Pläne an die tägliche Firmenroutine und den Arbeitsstil eines jeden Angestellten anzupassen. Die Tasks der Pläne werden systematisch so gestartet, dass kritische Daten als sicher geschützt bewahrt werden.

Die Möglichkeit zur Planung steht zur Verfügung, wenn Sie bei Erstellung eines Backup-Plans (S. 58) eines der folgenden Backup-Schemata verwenden: Einfach, Benutzerdefiniert oder 'Türme von Hanoi'. Sie können die Planungsmöglichkeit auch für Validierungstask (S. 266) einstellen.

Der Scheduler verwendet die lokale Zeit der Maschine, auf der der Backup-Plan existiert. Bevor Sie eine Planung erstellen, überprüfen Sie, ob die Datums- bzw. Zeit-Einstellungen der Maschine korrekt sind.

Planung

Sie müssen ein oder mehrere Ereignisse spezifizieren, um zu bestimmen, wann ein Task ausgeführt werden soll. Der Task wird gestartet, sobald eines der Ereignisse eintritt. Die Tabelle zeigt die unter Windows- und Linux-Betriebssystemen verfügbaren Ereignisse.

Ereignis	Windows	Linux
Zeit: Täglich, Wöchentlich, Monatlich	+	+
Verstrichene Zeit, seit das letzte erfolgreiche Backup abgeschlossen wurde. (geben Sie die Zeitdauer an)	+	+
Benutzeranmeldung (jeder Benutzer, aktueller Benutzer, geben Sie das Benutzerkonto an)	+	-
Benutzerabmeldung* (jeder Benutzer, aktueller Benutzer, geben Sie das Benutzerkonto an) *'Herunterfahren' ist nicht dieselbe Aktion wie 'Abmelden'. Der Task wird daher nicht beim Herunterfahren des Systems ausgeführt.	+	-
Systemstart	+	+
System herunterfahren	+	-
Ein Ereignis in der Windows-Ereignisanzeige (spezifizieren Sie die Parameter des Ereignisses)	+	-

Bedingung

Nur bei Backup-Aktionen können Sie zusätzlich zu den Ereignissen eine oder mehrere Bedingungen angeben. Sobald eines der Ereignisse eintritt, überprüft der Scheduler die Bedingung und führt den Task aus, falls die Bedingung erfüllt ist. Bei mehreren Bedingungen müssen diese alle gleichzeitig zusammentreffen, um die Task-Ausführung zu ermöglichen. Die Tabelle zeigt die unter Windows- und Linux-Betriebssystemen verfügbaren Bedingungen.

Bedingung: Task nur starten, wenn	Windows	Linux
Benutzer ist inaktiv (ein Bildschirmschoner ausgeführt wird oder die Maschine gesperrt ist)	+	-
Host des Speicherorts verfügbar ist	+	+
Laufzeit des Tasks sich innerhalb des spezifizierten Zeitintervalls befindet	+	+
Benutzer alle abgemeldet sind	+	-

Zeitperiode verstrichen ist, seit das letzte erfolgreiche Backup abgeschlossen wurde	+	+

Für den Fall, dass ein Ereignis eintritt, aber die Bedingung (oder eine von mehreren Bedingungen) nicht erfüllt ist, wird das Verhalten des Schedulers durch die Backup-Option Task-Startbedingungen (S. 141) definiert.

Was ist, wenn

- **Was ist, wenn ein Ereignis eintritt (und eine Bedingung, sofern vorhanden, erfüllt ist), während die Ausführung des vorherigen Tasks noch nicht abgeschlossen ist?**

  Das Ereignis wird ignoriert.

- **Was ist, wenn ein Ereignis eintritt, während der Scheduler auf die Bedingung wartet, die für das vorherige Ereignis benötigt wurde?**

  Das Ereignis wird ignoriert.

- **Was ist, wenn die Bedingung für eine sehr lange Zeit nicht erfüllt wird?**

  Wird die Verzögerung eines Backups zu riskant, so können Sie die Bedingung erzwingen (den Benutzer anweisen, sich abzumelden) oder den Task manuell ausführen. Sie können, damit diese Situation automatisiert gehandhabt wird, ein Zeitintervall definieren, nachdem der Task unabhängig von der Bedingung ausgeführt wird.

4.4.1 Tägliche Planung

Tägliche Planung ist für Windows- und Linux-Betriebssysteme wirksam.

So spezifizieren Sie eine tägliche Planung

Wählen Sie im Bereich **Planung** die passenden Parameter wie folgt:

Alle: <...> Tag(e)	Stellen Sie eine bestimmte Anzahl von Tagen ein, an denen Sie den Task ausgeführt haben wollen. Stellen Sie z.B. „Alle 2 Tage“ ein, so wird der Task an jedem zweiten Tag gestartet.

Wählen Sie im Bereich **Task-Ausführung während des Tages...** eine der folgenden Einstellungen:

Einmal um: <...>	Geben Sie den Zeitpunkt an, zu dem der Task einmalig ausgeführt wird.
Alle: <...> **Von: <...> Bis: <...>**	Stellen Sie ein, wie oft der Task während des angegebenen Zeitintervalls erneut gestartet wird. Stellen Sie z.B. die Task-Frequenz auf „Jede 1 Stunde“ von 10:00 Uhr bis 22:00 Uhr ein, so erlaubt dies dem Task, zwölfmal zu laufen: von 10:00 vormittags bis 22:00 abends innerhalb eines Tages.

Stellen Sie im Bereich **Wirksam...** Folgendes ein:

Von: <...>	Stellen Sie ein Datum ein, an dem diese Planung aktiviert wird (ein wirksames Datum). Wird dieses Kontrollkästchen deaktiviert, so wird der Task zum naheliegendsten, von Ihnen angegebenen Datum/Zeitpunkt gestartet.
Bis: <...>	Geben Sie ein Datum an, wann die Planung deaktiviert wird. Wird dieses Kontrollkästchen deaktiviert, so läuft der Task für eine unbegrenzte Anzahl von Tagen.

Erweiterte Planungseinstellungen (S. 98) sind nur für Maschinen verfügbar, die auf einem Acronis Backup & Recovery 11.5 Management Server registriert sind. Um diese Einstellungen zu spezifizieren, klicken Sie auf **Ändern** im Bereich **Erweiterte Einstellungen**.

Alle von Ihnen gemachten Einstellungen werden im Feld **Ergebnis** im unteren Teil des Fensters angezeigt.

Beispiele

„Einfache" tägliche Planung

Führe den Task jeden Tag um 18:00 Uhr aus.

Die Parameter der Planung werden wie folgt eingestellt:

1. Alle: **1** Tage.
2. Einmal: **18:00 Uhr**.
3. Wirksam:

   Von: **nicht eingestellt**. Der Task wird noch am selben Tag gestartet, sofern er vor 18:00 Uhr erstellt wurde. Wurde der Task nach 18:00 Uhr erstellt, dann wird er das erste Mal am nächsten Tag um 18:00 Uhr gestartet.

   Bis: **nicht eingestellt**. Der Task wird für eine unbegrenzte Zahl an Tagen ausgeführt.

„Drei-Stunden-Zeitintervall über drei Monate"-Planung

Den Task alle drei Stunden ausführen. Der Task startet an einem bestimmten Datum (z.B. 15. September 2009) und endet nach drei Monaten.

Die Parameter der Planung werden wie folgt eingestellt:

1. Alle: **1** Tage.
2. Alle: **3** Stunden

   Von: **24:00 Uhr** (Mitternacht) bis: **21:00 Uhr** – der Task wird daher achtmal pro Tag mit einem Intervall von 3 Stunden ausgeführt. Nach der letzten täglichen Wiederholung um 21:00 Uhr kommt der nächste Tag und der Task startet erneut von Mitternacht.
3. Wirksam:

   Von: **15.09.2009**. Wenn der 15.09.2009 das aktuelle Datum der Task-Erstellung ist und z.B. 13:15 Uhr die Erstellungszeit des Tasks, dann wird der Task gestartet, sobald das nächste Zeitintervall kommt: um 15:00 Uhr in unserem Beispiel.

   Bis: **15.12.2009**. An diesem Datum wird der Task das letzte Mal ausgeführt, der Task selbst ist jedoch immer noch in der Ansicht **Tasks** verfügbar.

Mehrere tägliche Planungen für einen Task

Es gibt Fälle, in denen es für Sie notwendig sein kann, den Task mehrmals am Tag laufen zu lassen oder sogar mehrmals am Tag mit unterschiedlichen Zeitintervallen. Erwägen Sie in diesen Fällen, einem Task mehrere Zeitplanungen hinzuzufügen.

Angenommen, der Task soll z.B. jeden dritten Tag ausgeführt werden, beginnend vom 20.09.2009, fünfmal am Tag:

- Zuerst um 8:00 Uhr.
- das zweite Mal um 12:00 Uhr (mittags)
- das dritte Mal um 15:00 Uhr
- das vierte Mal um 17:00 Uhr
- das fünfte Mal um 19:00 Uhr

Der offensichtliche Weg ist es, fünf einfache Zeitplanungen hinzuzufügen. Wenn Sie eine Minute überlegen, können Sie sich einen optimaleren Weg ausdenken. Wie Sie sehen, beträgt das Zeitintervall zwischen der ersten und zweiten Task-Wiederholung 4 Stunden und zwischen der

dritten, vierten und fünften sind es 2 Stunden. Für diesen Fall besteht die optimale Lösung darin, dem Task zwei Planungen hinzuzufügen.

Erste tägliche Planung

1. Alle: **3** Tage.
2. Alle: **4** Stunden.
   Von: **08:00:00 Uhr** bis: **12:00 Uhr**.
3. Wirksam:
   Von: **09/20/2009**.
   Bis: **nicht eingestellt**.

Zweite tägliche Planung

1. Alle: **3** Tage.
2. Alle: **2** Stunden.
   Von: **15:00 Uhr** bis: **19:00:00 Uhr**.
3. Wirksam:
   Von: **09/20/2009**.
   Bis: **nicht eingestellt**.

4.4.2 Wöchentliche Planung

Eine wöchentliche Planung ist für Windows- und Linux-Betriebssysteme wirksam.

So spezifizieren Sie eine wöchentliche Planung

Wählen Sie im Bereich **Planung** die passenden Parameter wie folgt:

Alle: <...> Woche (Wochen) am: <...>	Spezifizieren Sie eine gewisse Zahl von Wochen und die Wochentage, an denen Sie den Task ausführen wollen. Mit einer Einstellung z.B. alle **2** Wochen am **Montag** wird der Task am Montag jeder zweiten Woche ausgeführt.

Wählen Sie im Bereich **Task-Ausführung während des Tages...** eine der folgenden Einstellungen:

Einmal um: <...>	Geben Sie den Zeitpunkt an, zu dem der Task einmalig ausgeführt wird.
Alle: <...> **Von: <...> Bis: <...>**	Stellen Sie ein, wie oft der Task während des angegebenen Zeitintervalls gestartet wird. Eine Task-Frequenz von z.B. jede **1** Stunde von **10:00 Uhr** bis **22:00 Uhr** erlaubt es dem Task, während eines Tages 12-mal von 10:00 bis 22:00 Uhr zu laufen.

Stellen Sie im Bereich **Wirksam...** Folgendes ein:

Von: <...>	Stellen Sie ein Datum ein, an dem diese Planung aktiviert wird (ein wirksames Datum). Wird dieses Kontrollkästchen deaktiviert, so wird der Task zum naheliegendsten, von Ihnen angegebenen Datum/Zeitpunkt gestartet.
Bis: <...>	Geben Sie ein Datum an, wann die Planung deaktiviert wird. Wird dieses Kontrollkästchen deaktiviert, so läuft der Task für eine unbegrenzte Anzahl von Wochen.

Erweiterte Planungseinstellungen (S. 98) sind nur für Maschinen verfügbar, die auf einem Acronis Backup & Recovery 11.5 Management Server registriert sind. Um diese Einstellungen zu spezifizieren, klicken Sie auf **Ändern** im Bereich **Erweiterte Einstellungen**.

Alle von Ihnen gemachten Einstellungen werden im Feld **Ergebnis** im unteren Teil des Fensters angezeigt.

Beispiele

'Ein Tag in der Woche'-Planung

Den Task jeden Freitag um 22:00 Uhr ausführen, beginnend mit einem bestimmten Datum (z.B. 14.05.2009) und nach sechs Monaten endend.

Die Parameter der Planung werden wie folgt eingestellt:

1. Jeden: **1** Woche(n) am: **Fr**.
2. Einmal: **22:00:00 Uhr**.
3. Wirksam:

   Von: **13.05.2009**. Der Task wird am nächsten Freitag um 22:00 Uhr gestartet.

   Bis: **13.11.2009**. An diesem Datum wird der Task das letzte Mal ausgeführt, der Task selbst ist jedoch nach diesem Datum immer noch in der Task-Ansicht verfügbar. (Wenn dieser Tag kein Freitag wäre, dann würde der Task zuletzt an dem Freitag ausgeführt werden, der vor diesem Datum liegt.)

Diese Planung ist bei Erstellung benutzerdefinierter Backup-Schemata weit verbreitet. Die 'Ein Tag in der Woche'-Planung wird den Voll-Backups hinzugefügt.

'Werktags'-Planung

Den Task jede Woche an Werktagen ausführen: von Montag bis Freitag. Während eines Werktags startet der Task nur einmal um 21:00 Uhr.

Die Parameter der Planung werden wie folgt eingestellt:

1. Alle: **1** Woche(n) am: **<Werktags>** – die Wahl des Kontrollkästchens <Werktags> aktiviert automatisch die korrespondierenden Kontrollkästchen (**Mo**, **Di**, **Mi**, **Do** und **Fr**) und lässt die verbliebenen unverändert.
2. Einmal: **21:00 Uhr**.
3. Wirksam:

   Von: **leer**. Wenn Sie den Task z.B. am Montag um 11:30 Uhr erstellt haben, dann wird er am selben Tag um 21:00 Uhr gestartet. Wurde der Task z.B. am Freitag nach 21:00 Uhr erstellt, dann wird er das erste Mal am nächsten Wochentag (in unserem Beispiel Montag) um 21:00 Uhr gestartet.

   Enddatum: **leer**. Der Task wird für eine unbegrenzte Anzahl an Wochen erneut gestartet.

Diese Planung ist bei Erstellung benutzerdefinierter Backup-Schemata weit verbreitet. Die „Wochentags“-Planung wird den inkrementellen Backups hinzugefügt, während das Voll-Backup mit einer Ausführung an einem Tag in der Woche geplant wird. Zu weiteren Details siehe die Beispiele über vollständige und inkrementelle Backups sowie Bereinigungen im Abschnitt Benutzerdefiniertes Backup-Schema (S. 74).

Mehrere wöchentliche Planungen für einen Task

In Fällen, in denen der Task an verschiedenen Tagen der Woche mit verschiedenen Zeitintervallen ausgeführt werden muss, sollten Sie erwägen, jedem gewünschten Tag oder mehreren Tagen der Woche eine geeignete Planung zuzuweisen.

Angenommen, Sie müssen den Task mit der folgenden Planung ausführen:

- Montag zweimal, um 12:00 Uhr (mittags) und 21:00 Uhr
- Dienstag: alle 3 Stunden, von 9:00 bis 21:00 Uhr

- Mittwoch: alle 3 Stunden, von 9:00 bis 21:00 Uhr
- Donnerstag: alle 3 Stunden, von 9:00 bis 21:00 Uhr
- Freitag: zweimal, um 12:00 Uhr und 21:00 Uhr (d.h. wie am Montag)
- Samstag: einmal um 21:00 Uhr
- Sonntag: einmal um 21:00 Uhr

Durch Kombinieren der identischen Zeiten können die folgenden drei Planungen dem Task hinzugefügt werden:

Erste Planung

1. Alle: **1** Woche(n) am: **Mo**, **Fr**.
2. Alle: **9** Stunden
   Von: **12:00 Uhr** bis: **21:00 Uhr**.
3. Wirksam:
   Von: **nicht eingestellt**.
   Bis: **nicht eingestellt**.

Zweite Planung

1. Alle **1** Woche(n) am: **Di**, **Mi**, **Do**.
2. Alle **3** Stunden
   Von **09:00 Uhr** bis **21:00 Uhr**.
3. Wirksam:
   Von: **nicht eingestellt**.
   Bis: **nicht eingestellt**.

Dritte Planung

1. Alle: **1** Woche(n) am: **Sa, So**.
2. Einmal: **21:00 Uhr**.
3. Wirksam:
   Von: **nicht eingestellt**.
   Bis: **nicht eingestellt**.

4.4.3 Monatliche Planung

Eine monatliche Planung ist für Windows- und Linux-Betriebssysteme wirksam.

So spezifizieren Sie eine monatliche Planung

Wählen Sie im Bereich **Planung** die passenden Parameter wie folgt:

Monate: <...>	Wählen Sie den/die Monat(e), in der/denen Sie den Task ausführen wollen.
Tage: <...>	Bestimmen Sie die spezifischen Tage des Monats, um an diesen den Task auszuführen. Sie können außerdem den letzten Tag eines Monats auswählen, unabhängig von seinem tatsächlichem Datum.
Am(Um): <...> <...>	Bestimmen Sie die spezifischen Tage der Wochen, um an diesen den Task auszuführen.

Wählen Sie im Bereich **Task-Ausführung während des Tages...** eine der folgenden Einstellungen:

Einmal um: <...>	Geben Sie den Zeitpunkt an, zu dem der Task einmalig ausgeführt wird.

Alle: <...> **Von: <...> Bis: <...>**	Stellen Sie ein, wie oft der Task während des angegebenen Zeitintervalls gestartet wird. Eine Task-Frequenz von z.B. jede **1** Stunde von **10:00 Uhr** bis **22:00 Uhr** erlaubt es dem Task, während eines Tages 12-mal von 10:00 bis 22:00 Uhr zu laufen.

Stellen Sie im Bereich **Wirksam...** Folgendes ein:

Von: <...>	Stellen Sie ein Datum ein, an dem diese Planung aktiviert wird (ein wirksames Datum). Wird dieses Kontrollkästchen deaktiviert, so wird der Task zum naheliegendsten, von Ihnen angegebenen Datum/Zeitpunkt gestartet.
Bis: <...>	Geben Sie ein Datum an, wann die Planung deaktiviert wird. Wird dieses Kontrollkästchen deaktiviert, so läuft der Task für eine unbegrenzte Anzahl von Monaten.

Erweiterte Planungseinstellungen (S. 98) sind nur für Maschinen verfügbar, die auf einem Acronis Backup & Recovery 11.5 Management Server registriert sind. Um diese Einstellungen zu spezifizieren, klicken Sie auf **Ändern** im Bereich **Erweiterte Einstellungen**.

Alle von Ihnen gemachten Einstellungen werden im Feld **Ergebnis** im unteren Teil des Fensters angezeigt.

Beispiele

„Letzter Tag eines jeden Monats"-Planung

Den Task einmal um 22:00 Uhr am letzten Tag eines jeden Monats ausführen.

Die Parameter der Planung werden wie folgt eingestellt:

1. Monate: **<Alle Monate>**.
2. Tage: **Letzter**. Der Task wird am letzten Tag eines jeden Monats ausgeführt, ungeachtet seines tatsächlichen Datums.
3. Einmal: **22:00:00 Uhr**.
4. Wirksam:

   Von: **leer**.

   Bis: **leer**.

Diese Planung ist bei Erstellung benutzerdefinierter Backup-Schemata weit verbreitet. Die „Letzter Tag eines jeden Monats"-Planung wird den Voll-Backups hinzugefügt, während die differentiellen Backups zur einmaligen Ausführung pro Woche und inkrementelle an Wochentagen geplant werden. Zu weiteren Details siehe die Beispiele über monatliche vollständige, wöchentliche differentielle und tägliche inkrementelle Backups sowie zu Bereinigung im Abschnitt Benutzerdefiniertes Backup-Schema (S. 74).

„Jahreszeiten"-Planung

Den Task an allen Werktagen während der nördlichen Herbst-Jahreszeit von 2009 und 2010 ausführen. Während eines Werktages wird der Task alle 6 Stunden von 0:00 (Mitternacht) bis 18:00 Uhr gestartet.

Die Parameter der Planung werden wie folgt eingestellt:

1. Monate: **September, Oktober, November**.
2. Am(Um): **<alle> <Werktage>**.
3. Alle: **6** Stunden.

   Von: **00:00 Uhr** bis: **18:00:00 Uhr**.

4. Wirksam:

   Von: **30.08.2009**. Tatsächlich wird der Task am ersten Werktag des Septembers gestartet. Durch Einstellung dieses Datums bestimmen Sie lediglich, dass der Task in 2009 gestartet werden muss.

   Bis: **01.12.2010**. Tatsächlich wird der Task am letzten Werktag des Novembers enden. Durch Einstellung dieses Datums bestimmen Sie lediglich, dass der Task in 2010 nicht fortgesetzt werden darf, nachdem der Herbst in der nördlichen Hemisphäre endet.

Mehrere monatliche Planungen für einen Task

In Fällen, in denen der Task an verschiedenen Tagen oder Wochen mit verschiedenen, vom Monat abhängigen Zeitintervallen ausgeführt werden muss, sollten Sie erwägen, jedem gewünschten Monat oder mehreren Monaten eine geeignete Planung zuzuweisen.

Angenommen, der Task tritt am 01.11.2009 in Kraft.

- Während des nördlichen Winters läuft der Task einmal um 22:00 Uhr an jedem Werktag.
- Während des nördlichen Frühlings und Herbstes läuft der Task alle 12 Stunden an allen Werktagen.
- Während des nördlichen Sommers läuft der Task an jedem 1. und 15. eines Monats um 22:00 Uhr.

Somit werden die folgenden drei Planungen dem Task hinzugefügt:

Erste Planung

1. Monate: **Dezember**, **Januar**, **Februar**.
2. Am(Um): **<Alle> <An allen Werktagen>.**
3. Einmal: **22:00:00 Uhr**.
4. Wirksam:

   Von: **11/01/2009**.

   Bis: **nicht eingestellt**.

Zweite Planung

1. Monate: **März**, **April**, **Mai**, **September**, **Oktober**, **November**.
2. Am(Um): **<Alle> <An allen Werktagen>**.
3. Alle: **12 Stunden**

   Von: **00:00 Uhr** bis: **12:00 Uhr**.
4. Wirksam:

   Von: **11/01/2009**.

   Bis: **nicht eingestellt**.

Dritte Planung

1. Monate: **Juni**, **Juli**, **August**.
2. Tage: **1**, **15**.
3. Einmal: **22:00:00 Uhr**.
4. Wirksam:

   Von: **11/01/2009**.

   Bis: **nicht eingestellt**.

4.4.4 Bei Ereignis in der Windows-Ereignisanzeige

Diese Art der Planung ist nur in Windows-Betriebssystemen wirksam.

Sie können einen Backup-Task so planen, dass er gestartet wird, wenn ein bestimmtes Windows-Ereignis in eine der Protokolllisten (Anwendungen, Sicherheit oder System) aufgenommen wird.

Angenommen, Sie wollen einen Backup-Plan aufstellen, der automatisch ein vollständiges Notfall-Backup Ihrer Daten durchführt, sobald Windows entdeckt, dass die Festplatte vor einem Ausfall steht.

Parameter

Protokollname

Spezifizieren Sie den Namen eines Protokolls. Wählen Sie den Namen einer Standard-Protokollliste (**Anwendung**, **Sicherheit** oder **System**) oder geben Sie den Namen einer Protokollliste ein – beispielsweise: **Microsoft Office Sitzungen**

Ereignisquelle

Spezifizieren Sie die Quelle des Ereignisses, welche typischerweise das Programm oder die Systemkomponente angibt, die das Ereignis verursachte – beispielsweise: **disk**

Ereignistyp

Geben Sie den Typ des Ereignisses an: **Fehler**, **Warnung**, **Informationen**, **Überprüfung erfolgreich** oder **Überprüfung fehlgeschlagen**.

Ereignis-Kennung:

Bezeichnet die Ereignis-Nummer, die üblicherweise die spezielle Art der Ereignisse unter Ereignissen derselben Quelle identifiziert.

So tritt z.B. ein **Fehler**-Ereignis mit der Ereignisquelle **disk** und der Ereignis-Kennung **7** auf, wenn Windows einen fehlerhaften Block auf einer Festplatte entdeckt, während ein **Fehler**-Ereignis mit der Ereignisquelle **disk** und der Ereignis-Kennung **15** stattfindet, wenn eine Festplatte noch nicht zugriffsbereit ist.

Beispiele

„Fehlerhafte Blöcke"-Notfall-Backup

Treten ein oder mehrere fehlerhafte Blöcke plötzlich auf einer Festplatte auf, so deutet das üblicherweise auf einen baldigen Ausfall der Festplatte hin. Angenommen, Sie wollen einen Backup-Plan erstellen, der die Daten einer Festplatte sichert, sobald eine solche Situation eintritt:

Wenn Windows einen fehlerhaften Block auf einer Festplatte entdeckt, nimmt es ein Ereignis mit der Ereignis-Quelle **disk** und der Ereignis-Kennung **7** in die Protokollliste **System** auf; der Typ des Ereignisses ist **Fehler**.

Wenn Sie den Plan erstellen, geben Sie Folgendes im Bereich **Planung** ein bzw. wählen es aus:

- **Protokollname**: **System**
- **Ereignis-Quelle**: **disk**
- **Ereignis-Typ**: **Fehler**
- **Ereignis-Kennung**: **7**

Wichtig: *Um sicherzustellen, dass ein solcher Task trotz Vorhandenseins der fehlerhaften Blöcke fertiggestellt wird, müssen Sie angeben, dass der Task diese ignoriert. Zur Umsetzung gehen Sie in den **Backup-Optionen** zum Unterpunkt **Fehlerbehandlung** und aktivieren das Kontrollkästchen **Fehlerhafte Sektoren ignorieren**.*

Vor-Update-Backup in Windows Vista

Angenommen Sie wollen einen Backup-Plan erstellen, der automatisch ein Backup des Systems durchführt – z.B. durch Sicherung der Partition, auf der Windows installiert ist – jedes Mal, wenn Windows davor steht, Updates zu installieren.

Nach dem Download eines oder mehrerer Updates und Planung der Installation nimmt Windows Vista ein Ereignis mit der Quelle **Microsoft-Windows-WindowsUpdateClient** und der Ereignis-Nummer **18** in die Protokollliste **System** auf; der Typ dieses Ereignisses ist **Informationen**.

Wenn Sie den Plan erstellen, geben Sie Folgendes im Bereich **Planung** ein bzw. wählen es aus:

- **Protokollname**: **System**
- **Ereignis-Quelle**: **Microsoft-Windows-WindowsUpdateClient**
- **Ereignis-Typ**: **Informationen**
- **Ereignis-Kennung**: **18**

Tipp: *Um einen vergleichbaren Backup-Plan für unter Windows XP laufende Maschinen aufzusetzen, ersetzen Sie den Text in **Ereignis-Quelle** mit **Windows Update Agent** und lassen Sie die übrigen Felder gleich.*

So können Sie Ereignisse in der Ereignisanzeige einsehen

So öffnen Sie eine Meldung in der Ereignisanzeige

1. Klicken Sie auf dem Desktop oder im **Start-**Menü mit der rechten Maustaste auf **Computer** und dann im Kontextmenü auf **Verwalten**.
2. Erweitern Sie in der Konsole **Computerverwaltung** den Zweig **System** und dann **Ereignisanzeige**.
3. Klicken Sie in der **Ereignisanzeige** auf den Namen einer Protokollliste, die Sie einsehen wollen – z.B. **Anwendung**.

   Hinweis: *Um die Sicherheitsprotokollliste öffnen zu können (**Sicherheit**), müssen Sie Mitglied der Gruppe „Administratoren" sein.*

So können Sie die Eigenschaften eines Ereignisses einsehen, inklusive seiner Quelle und Nummer (Ereigniskennung).

1. Klicken Sie in der **Ereignisanzeige** auf den Namen einer Protokollliste, die Sie einsehen wollen – z.B. **Anwendung**.

   Hinweis: *Um die Sicherheitsprotokollliste öffnen zu können (**Sicherheit**), müssen Sie Mitglied der Gruppe „Administratoren" sein.*

2. Klicken Sie im rechten Fensterbereich der Protokollliste auf den Namen des Ereignisses, dessen Eigenschaften Sie sehen wollen.
3. Im Dialogfenster **Eigenschaften** sehen Sie alle Informationen des Ereignisses, wie etwas seinen Ursprung im Feld **Quelle**, und seine Nummer, die im Feld **Ereignis-Kennung** angezeigt wird.

Sind Sie fertig, so klicken Sie auf **OK**, um das Dialogfenster **Eigenschaften** zu schließen.

4.4.5 Erweiterte Planungseinstellungen

Die folgenden erweiterten Einstellungen sind verfügbar, wenn Sie in einem zentralen Backup-Plan eine tägliche, wöchentliche oder monatliche Planung konfigurieren.

Wake-on-LAN verwenden

Wenn diese Einstellung aktiviert ist, verwendet der Acronis Backup & Recovery 11.5 Management Server die Wake-on-LAN-Funktion, um ausgeschaltete, registrierte Maschinen aufzuwecken, wenn die geplante Startzeit für ein Backup, eine Bereinigung oder eine Validierung erreicht ist. Wenn der Backup-Task auf den einzelnen Maschinen mit Verzögerung gestartet wird (siehe die nächste Einstellung), dann weckt der Management Server die Maschinen entsprechend dieser Verzögerungen auf.

Bevor Sie diese Einstellung verwenden, vergewissern Sie sich, dass Sie Wake-on-LAN auf den registrierten Maschinen aktiviert haben. Die BIOS-Konfiguration der Maschine, die Konfiguration des Netzwerkadapters und die Konfiguration des Betriebssystems müssen so sein, dass die Maschine aus dem „Soft-Off"-Zustand – auch als Energiezustand S5 oder G2 bekannt – aufgeweckt werden kann.

Startzeit innerhalb des Zeitfensters verteilen

Wenn diese Einstellung aktiviert ist, startet der Backup-Task auf jeder registrierten Maschine mit einer bestimmten Verzögerung zu der im Backup-Plan eingestellten Startzeit. Dadurch werden die tatsächlichen Startzeiten des Tasks im Zeitintervall verteilt.

Möglicherweise möchten Sie diese Einstellung verwenden, wenn Sie einen zentralen Backup-Plan zur Ausführung von Backups für mehrere Maschinen auf einem Netzwerkspeicherort erstellen, um eine übermäßige Netzwerklast zu vermeiden.

Die Verzögerungswerte reichen von Null bis zur angegebenen maximalen Verzögerung und sie werden entsprechend der ausgewählten Verteilungsmethode bestimmt. Der Verzögerungswert für jede Maschinen wird bestimmt, wenn der Backup-Plan auf die Maschine bereitgestellt wird und er bleibt so lange gleich, bis Sie den Backup-Plan bearbeiten und den maximalen Verzögerungswert ändern.

Die Bedingungen werden, falls vorhanden, zur tatsächlichen Startzeit eines Tasks auf den einzelnen Maschinen überprüft.

Unabhängig vom maximalen Verzögerungswert bleiben alle Startzeiten innerhalb desselben Datums. Startet Ihr Backup-Plan beispielsweise um 23:00 Uhr und beträgt der maximale Verzögerungswert zwei Stunden, dann liegen die Startzeiten aller Tasks dennoch nur zwischen 23:00 und 23:59 Uhr. Die Tasks können aber, wie üblich, nach Mitternacht abgeschlossen werden.

Das folgende Beispiel veranschaulicht diese Einstellung.

Beispiel 1

Angenommen, Sie stellen einen zentralen Backup-Plan auf drei Maschinen mit folgender Planung bereit:

Task starten: **Täglich**
Einmal um: **09:00:00 Uhr**

Startzeit innerhalb des Zeitfensters verteilen
Maximale Verzögerung: **1 Stunde**
Verteilungsmethode: **Zufällig**

In diesem Fall kann die Startzeit des Tasks auf jeder Maschinen ein beliebiger Zeitpunkt zwischen 09:00:00 Uhr und 09:59:59 Uhr sein; beispielsweise:

Erste Maschine: Jeden Tag um 09:30:03 Uhr

Zweite Maschine: Jeden Tag um 09:00:00 Uhr

Dritte Maschine: Jeden Tag um 09:59:59 Uhr

Beispiel 2

Angenommen, Sie stellen einen zentralen Backup-Plan auf drei Maschinen mit folgender Planung bereit:

Task starten: **Täglich**
Alle: **2 Stunden** Von: **09:00:00 Uhr** Bis: **11:00:00 Uhr**

Startzeit innerhalb des Zeitfensters verteilen
Maximale Verzögerung: **1 Stunde**
Verteilungsmethode: **Zufällig**

In diesem Fall kann der Zeitpunkt, an dem der Task erstmalig auf jeder Maschine ausgeführt wird, ein beliebiger Zeitpunkt zwischen 09:00:00 Uhr und 09:59:59 Uhr sein. Die Zeit zwischen der ersten und der zweiten Ausführung beträgt exakt zwei Stunden. Zum Beispiel:

Erste Maschine: Jeden Tag um 09:30:03 Uhr und um 11:30:03 Uhr

Zweite Maschine: Jeden Tag um 09:00:00 Uhr und um 11:00:00 Uhr

Dritte Maschine: Jeden Tag um 09:59:59 Uhr und um 11:59:59 Uhr

Erweiterte Einstellungen spezifizieren

1. Verbinden Sie sich mit dem Management Server und starten Sie dann mit der Erstellung eines Backup-Plans.
2. Wählen Sie bei **Art des Backups** das Backup-Schema **Einfach**, **GVS (Großvater-Vater-Sohne)**, **Türme von Hanoi** oder **Benutzerdefiniert**.
3. Gehen Sie, abhängig vom Backup-Schema, folgendermaßen vor:
   - Klicken Sie beim Backup-Schema **GVS (Großvater-Vater-Sohn)** auf **Erweiterte Einstellungen**.
   - Beim Backup-Schema **Einfach**, **Türme von Hanoi** oder **Benutzerdefiniert**:
   a. Klicken Sie auf **Planung**, um eine Planung für das Schema zu spezifizieren.
   b. Wählen Sie unter **Task starten** die Option **Täglich**, **Wöchentlich** oder **Monatlich** aus.
   c. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Ändern**.
4. Wenn Sie die Verwendung der Wake-on-LAN-Funktion ermöglichen möchten, aktivieren Sie das Kontrollkästchen **Wake-on-LAN verwenden**.
5. Wenn Sie die Startzeiten der zentralen Backup-Tasks verteilen möchten, aktivieren Sie das Kontrollkästchen **Startzeit innerhalb des Zeitfensters verteilen** und geben Sie dann den maximalen Verzögerungswert und die Verteilungsmethode an.

4.4.6 Bedingungen

Bedingungen erweitern den Scheduler mit mehr Flexibilität und ermöglichen es, Backup-Tasks abhängig von gewissen Bedingungen auszuführen. Sobald ein spezifiziertes Ereignis eintritt (siehe den Abschnitt 'Planung (S. 89)' zur Liste verfügbarer Ereignisse), überprüft der Scheduler die angegebene Bedingung und führt den Task aus, sofern die Bedingung zutrifft.

Bedingungen sind nur bei Verwendung des benutzerdefinierten Backup-Schemas (S. 74) verfügbar. Bedingungen können für vollständige, inkrementelle und differentielle Backups separat konfigurieren werden.

Für den Fall, dass ein Ereignis eintritt, aber die Bedingung (oder eine von mehreren Bedingungen) nicht erfüllt ist, wird das Verhalten des Schedulers durch die Backup-Option **Task-Startbedingungen** (S. 141) definiert. Dort können Sie angeben, wie wichtig die Bedingungen für die Backup-Strategie sind:

- Bedingungen sind zwingend – setzt die Ausführung des Backup-Tasks auf Wartestellung, bis alle Bedingungen zutreffen.

- Bedingungen sind wünschenswert, aber die Ausführung eines Backup-Tasks hat höhere Priorität – setzt den Task für das angegebene Zeitintervall auf Wartestellung. Wenn das Zeitintervall vergeht und die Bedingungen immer noch nicht zutreffen, führe den Task auf jeden Fall aus. Mit dieser Einstellung handhabt das Programm automatisch Situationen, wenn Bedingungen eine zu lange Zeit nicht zutreffen und eine weitere Verzögerung des Backups unerwünscht ist.
- Startzeit des Backup-Tasks ist relevant – überspringe den Backup-Tasks, wenn die Bedingungen zu dem Zeitpunkt, wenn der Task gestartet werden soll, nicht zutreffen. Ein Überspringen der Task-Ausführung macht Sinn, wenn Sie Daten ganz genau zur angegebenen Zeit sichern müssen, insbesondere, wenn die Ereignisse relativ häufig sind.

Mehrere Bedingungen hinzufügen

Sollten zwei oder mehr Bedingungen spezifiziert sein, dann wird das Backup nur starten, wenn alle davon erfüllt sind.

4.4.6.1 Benutzer ist untätig

Gilt für: Windows

„Benutzer ist untätig" bedeutet, dass auf der verwalteten Maschine ein Bildschirmschoner läuft oder die Maschine gesperrt ist.

Beispiel:

Starte den Backup-Task auf der verwalteten Maschine täglich um 21:00 Uhr, möglichst, wenn der Benutzer untätig ist. Ist der Benutzer um 23 Uhr immer noch aktiv, starte den Task dennoch.

- Ereignis: **Täglich**, alle **1** Tage; einmal um: **09:00:00 PM**.
- Bedingung: **Benutzer ist untätig**.
- Task-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**, den Task dennoch starten nach **2** Stunde(n).

Ergebnis:

(1) Wenn der Benutzer vor 21 Uhr untätig wird, startet der Backup-Task um 21 Uhr.

(2) Wenn der Benutzer zwischen 21 und 23 Uhr untätig wird, startet der Backup-Task sofort, nachdem der Benutzer untätig wurde.

(3) Wenn der Benutzer um 23 Uhr immer aktiv ist, startet der Backup-Task dennoch.

4.4.6.2 Host des Speicherorts verfügbar ist

Gilt für: Windows, Linux

„Host des Speicherorts ist verfügbar" bedeutet, dass die Maschine, die das Ziel zum Speichern von Archiven auf einem Netzlaufwerk bereithält, verfügbar ist.

Beispiel:

Eine Datensicherung zu einem Netzwerk-Speicherort wird werktags um 21:00 Uhr durchgeführt. Wenn der Speicherort des Hosts zu dem Zeitpunkt nicht verfügbar ist (z.B. wegen Wartungsarbeiten), überspringe das Backup und warte bis zum nächsten Werktag, um den Task zu starten. Es wird angenommen, dass der Backup-Task besser überhaupt nicht gestartet werden soll, statt fehlzuschlagen.

- Ereignis: **Wöchentlich**, alle **1** Woche(n) an **<Werktagen>**; einmal um **21:00 Uhr**.

- Bedingung: **Host des Speicherorts verfügbar ist**
- Task-Startbedingungen: **Ausführung des Tasks übergehen**.

Ergebnis:

(1) Wenn es 21:00 Uhr wird und der Host des Speicherorts verfügbar ist, startet der Backup-Task zur rechten Zeit.

(2) Wenn es 21:00 Uhr wird, der Host im Augenblick aber nicht verfügbar ist, dann startet der Backup-Task am nächsten Werktag, sofern der Host des Speicherorts dann verfügbar ist.

(3) Wenn der Host des Speicherorts an Werktagen um 21:00 Uhr niemals verfügbar ist, startet auch der Task niemals.

4.4.6.3 Entspricht Zeitintervall

Gilt für: Windows, Linux

Beschränkt die Startzeit eines Backup-Tasks auf ein angegebenes Zeitintervall.

Beispiel

Eine Firma verwendet unterschiedliche Speicherorte auf demselben netzwerkangebundenen Speicher zur Sicherung von Benutzerdaten und Servern. Der Arbeitstag startet um 8:00 und endet um 17:00 Uhr. Die Benutzerdaten sollen gesichert werden, sobald der User sich abmeldet, aber nicht vor 16:30 Uhr und nicht später als 22:00 Uhr. Die Firmen-Server werden jeden Tag um 23:00 Uhr per Backup gesichert. Daher sollten alle Daten der Benutzer vorzugsweise vor dieser Zeit gesichert werden, um Netzwerk-Bandbreite frei zu machen. Indem Sie das obere Limit auf 22:00 Uhr setzen, wird angenommen, dass die Sicherung der Benutzerdaten nicht länger als eine Stunde benötigt. Wenn ein Benutzer innerhalb des angegebenen Zeitintervalls noch angemeldet ist oder sich zu irgendeiner anderen Zeit abmeldet – sichere keine Benutzerdaten, d.h. überspringe die Task-Ausführung.

- Ereignis: **Beim Abmelden**, Der folgende Benutzer: **Jeder Benutzer**.
- Bedingung: **Entspricht dem Zeitintervall** von **16:30 Uhr** bis **22:00 Uhr**.
- Task-Startbedingungen: **Ausführung des Tasks übergehen**.

Ergebnis:

(1) Wenn sich der Benutzer zwischen 16:30 Uhr und 22:00 Uhr abmeldet, wird der Backup-Task unmittelbar nach der Abmeldung gestartet.

(2) Wenn sich der Benutzer zu einer anderen Zeit abmeldet, wird der Task übersprungen.

Was ist, wenn...

Was ist, wenn ein Task-Ausführung für einen bestimmten Zeitpunkt geplant ist und dieser außerhalb des spezifizierten Zeitintervalls liegt?

Ein Beispiel:

- Ereignis: **Täglich**, alle **1** Tage; einmal um **15:00 Uhr**.
- Bedingung: **Entspricht dem Zeitintervall** von **18:00 Uhr** bis **23:59:59 Uhr**.

In diesem Fall hängt die Antwort auf die Frage, ob und wann der Task ausgeführt wird, von den Task-Startbedingungen ab:

- Wenn die Task-Startbedingungen **Ausführung des Tasks übergehen** lauten, dann wird der Task niemals laufen.
- Wenn die Task-Startbedingungen **Warten, bis die Bedingungen erfüllt sind** lauten und das Kontrollkästchen **Task trotzdem ausführen nach** *deaktiviert* ist, wird der Task (für 15:00 Uhr geplant) um 18:00 Uhr gestartet — dem Zeitpunkt, wenn die Bedingung erfüllt ist.
- Wenn die Task-Startbedingungen **Warten, bis die Bedingungen erfüllt sind** lauten und das Kontrollkästchen **Task trotzdem ausführen nach** mit z.B. einer Wartezeit von **1 Stunde** *aktiviert* ist, wird der Task (für 15:00 Uhr geplant) um 16:00 Uhr gestartet — dem Zeitpunkt, zu dem die Warteperiode endet.

4.4.6.4 Benutzer ist abgemeldet

Gilt für: Windows

Ermöglicht Ihnen, einen Backup-Task auf Warteposition zu setzen, bis sich alle Benutzer auf der verwalteten Maschine von Windows abgemeldet haben.

Beispiel

Führe den Backup-Task um 20:00 Uhr am ersten und dritten Freitag eines jeden Monats aus, möglichst, wenn alle Benutzer abgemeldet sind. Sollte einer der Benutzer um 23:00 Uhr immer noch angemeldet sein, führe den Task dennoch aus.

- Ereignis: **Monatlich**, Monate: **<Alle>**; An: **<Erster>**, **<Dritter> <Freitag>**; einmalig um **20:00 Uhr**.
- Bedingung: **Benutzer sind abgemeldet**.
- Task-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**, den Task dennoch starten nach **3** Stunde(n).

Ergebnis:

(1) Wenn alle Benutzer um 20:00 Uhr abgemeldet sind, startet der Backup-Task um 20:00 Uhr.

(2) Wenn sich der letzte Benutzer zwischen 20:00 und 23:00 Uhr abmeldet, wird der Backup-Task sofort ausgeführt, nachdem sich der Benutzer abgemeldet hat.

(3) Wenn ein Benutzer um 23:00 Uhr immer noch angemeldet ist, startet der Backup-Task dennoch.

4.4.6.5 Zeit seit letztem Backup

Gilt für: Windows, Linux

Ermöglicht Ihnen, einen Backup-Task auf Warteposition zu setzen, bis das angegebene Zeitintervall verstreicht, seit das letzte Backup erfolgreich fertiggestellt wurde.

Beispiel:

Den Backup-Task bei Systemstart ausführen, aber nur, wenn mehr als 12 Stunden seit dem letzten erfolgreichen Backup verstrichen sind.

- Ereignis: **Beim Start**, führt den Task beim Starten der Maschine aus.
- Bedingung: **Zeit seit dem letzten Backup**, Zeit seit dem letzten Backup: **12** Stunden.
- Task-Startbedingungen: **Warten, bis die Bedingungen erfüllt sind**.

Ergebnis:

(1) Wenn die Maschine neu gestartet wird, bevor seit Abschluss des letzten erfolgreichen Backup 12 Stunden verstrichen sind, dann wird der Scheduler warten, bis die 12 Stunden abgelaufen sind und dann den Task starten.

(2) Wenn die Maschine mindestens 12 Stunden nach Abschluss des letzten erfolgreichen Backups neu gestartet wird, dann wird der Backup-Task direkt ausgeführt.

(3) Wenn die Maschine niemals neu gestartet wird, wird auch der Task niemals ausgeführt. Sie können das Backup in der Ansicht **Backup-Pläne und Tasks** manuell starten, falls das nötig ist.

4.5 Replikation und Aufbewahrung von Backups

Bei Erstellung eines Backup-Plans (S. 58) spezifizieren Sie den primären Speicherort für die Backups. Zusätzlich können Sie Folgendes tun:

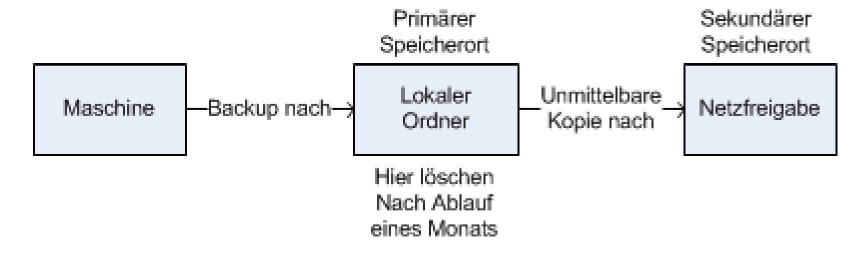
- Jedes Backup als 'Replikat' direkt nach seiner Erstellung zu einem zweiten Speicherort kopieren lassen.
- Die Backups entsprechend der von Ihnen spezifizierten Aufbewahrungsregeln bewahren und sie dann entweder zu einem zweiten Speicherort zu verschieben oder sie zu löschen.

Auf ähnliche Weise können Sie Backups von einem zweiten Speicherort zu einem dritten kopieren oder verschieben (usw.). Es werden bis zu fünf aufeinanderfolgende Speicherorte unterstützt (den ersten eingeschlossen).

Hinweis: *Die Replikationsfunktion ersetzt und erweitert die Option* ***Dual Destination****, die in Acronis Backup & Recovery 10 verfügbar war.*

Beispiel: Sie erstellen ein Backup Ihrer Maschine in einen lokalen Ordner. Das Backup wird unmittelbar in einen Netzwerkordner kopiert. Das Backup wird im ursprünglichen lokalen Ordner nur für einen Monat gespeichert.

Das folgende Bild illustriert dieses Beispiel.



Einsatzszenarien

- **Verlässliches Desaster-Recovery** (S. 110)

  Speichern Sie Ihre Backups sowohl 'on-site' (zur sofortigen Wiederherstellung) wie auch 'off-site' (um die Backups vor Ausfall des lokalen Speichers oder natürlichen Desastern zu schützen).
- **Nur die jüngsten Recovery-Punkte bewahren** (S. 111)

  Löschen Sie ältere Backups von einem schnellen Speicher gemäß den Aufbewahrungsregeln, um teuren Speicherplatz nicht übermäßig zu beanspruchen.
- **Reduzierte Kosten bei der Speicherung von Backups** (S. 112)

  Speichern Sie Ihre Backups solange auf einem schnellen Speicher, wie es wahrscheinlich ist, dass Sie auf diese Daten zugreifen müssen. Verschieben Sie sie danach auf einen Speicher mit niedrigeren Kosten, um Sie dort für einen längeren Zeitraum aufbewahren zu können. Das ermöglicht Ihnen auch, gesetzliche Bestimmungen zur Datenaufbewahrung einzuhalten.

- **Backup zu einem langsamen Gerät innerhalb eines engen Backup-Fensters** (S. 112)

  Lassen Sie die Backups über Nacht zu einem verwalteten Depot mit schnellem Speicher erstellen – und dann über Tag vom Acronis Backup & Recovery 11.5 Storage Node auf Bänder verschieben.
- **Die Acronis Cloud verwenden, um Daten vor einem natürlichen Desaster zu schützen** (S. 111)

  Replizieren Sie Archive zum Online Storage, indem lediglich Änderungen an den Daten außerhalb der üblichen Arbeitsstunden übertragen werden.

Replikation und Aufbewahrung in Backup-Schemata

Die nachfolgende Tabelle zeigt die Verfügbarkeit von Replikation und Aufbewahrungsregeln in verschiedenen Backup-Schemata.

Backup-Schema	Kann Backups kopieren	Kann Backups verschieben	Kann Backups löschen
Manueller Start (S. 79)	Ja	Nein	Nein
Einfach (S. 69)	Ja	Ja	Ja
GVS (Großvater-Vater-Sohn) (S. 70)	Ja	Nein	Ja
Türme von Hanoi (S. 76)	Ja	Nein	Ja
Benutzerdefiniert (S. 74)	Ja	Ja	Ja
Initial Seeding (S. 79)	Nein	Nein	Nein

Anmerkungen:

- Eine Konfiguration, bei der Backups vom selben Speicherort gleichermaßen kopiert und verschoben werden, ist nicht möglich.
- In Kombination mit der Option Vereinfachte Benennung von Backup-Dateien (S. 83) stehen weder Replikation noch Aufbewahrungsregeln zur Verfügung.

4.5.1 Unterstützte Speicherorte

Sie können ein Backup *von* jedem der nachfolgenden Speicherorte aus kopieren oder verschieben:

- Ein lokaler Ordner auf einem fest eingebauten Laufwerk
- Netzwerkordner
- FTP- oder SFTP-Server
- Acronis Backup & Recovery 11.5 Storage Node
- Acronis Secure Zone

Sie können ein Backup *zu* jedem der nachfolgenden Speicherorte kopieren oder verschieben:

- Ein lokaler Ordner auf einem fest eingebauten Laufwerk
- Netzwerkordner
- FTP- oder SFTP-Server
- Acronis Backup & Recovery 11.5 Storage Node
- Bandgeräte
- Acronis Online Backup Storage
- Ein Wechsellaufwerk (S. 221), welches im Modus **Eingebautes Laufwerk** verwendet wird. (Sie wählen beim Erstellen eines Backup-Plans den Wechsellaufwerkmodus.)

Backups, die zu einem nächsten Speicherort kopiert oder verschoben wurden, sind unabhängig von den Backups, die auf dem ursprünglichen Speicherort verbleiben (und umgekehrt). Sie können Daten von jedem dieser Backups wiederherstellen, ohne Zugriff auf andere Speicherorte.

Einschränkungen

- Kopieren oder Verschieben von Backups *auf und von* optischen Laufwerken (CD-, DVD-, Blu-ray-Medien) wird nicht unterstützt.
- Das Kopieren oder Verschieben von Backups *zu und von* Wechsellaufwerken, die im Modus **Wechselmedium** verwendet werden, wird nicht unterstützt.
- Kopieren oder Verschieben von Backups *von* einem Acronis Backup & Recovery 11.5 Storage Node *zu* einem lokalen Ordner wird nicht unterstützt. Mit 'lokaler Ordner' ist ein Ordner auf der Maschine mit dem Agenten gemeint, der das Backup erstellt hat.
- Ein Bandgerät und der Acronis Online Backup Storage kann je nur der finale Speicherort sein. Nachfolgendes Kopieren oder Verschieben von Backups *von* dort aus ist nicht möglich.
- Sie können denselben Speicherort nicht mehr als einmal spezifizieren. Sie können ein Backup beispielsweise nicht von einem Ordner zu einem anderen verschieben – und dann wieder zurück zum ursprünglichen Ordner.

Welche Maschine führt diese Aktion aus?

Kopieren, Verschieben oder Löschen eines Backups *von* einem Speicherort aus wird durch den Agenten initiiert, der das Backup erstellt hat – und wird durchgeführt:

- Von diesem Agenten, sofern der Speicherort *kein* verwaltetes Depot ist.
- Von dem korrespondierendem Storage Node, sofern der Speicherort *ein* verwaltetes Depot ist. Kopieren oder Verschieben eines Backups *von* einem verwalteten Depot *zum* Online Storage wird jedoch von dem Agenten durchgeführt, der das Backup erstellt hat.

Aus der oberen Erläuterung folgt, dass die Aktion nur durchgeführt wird, wenn die Maschine mit dem Agenten angeschaltet ist. Falls es sich um eine geplante Aktion handelt, verwendet die Planung die Datums- und Zeiteinstellungen dieser Maschine.

Kopieren und Verschieben von Backups zwischen verwalteten Depots

Das Kopieren oder Verschieben eines Backups von einem verwalteten Depot zu einem anderen verwalteten Depot wird vom Storage Node durchgeführt.

Sollt das Ziel-Depot ein deduplizierendes Depot (S. 488) sein (möglicherweise auf einem anderen Storage Node), dann sendet der als Quelle dienende Storage Node nur solche Datenblöcke, die auf dem als Ziel dienenden Depot noch nicht vorliegen. Anders ausgedrückt führt der Storage Node also (wie ein Agent) eine Deduplizierung an der Quelle (S. 260) durch. Das reduziert den Netzwerkverkehr, wenn Sie Daten zwischen örtlich getrennten Storage Nodes replizieren.

4.5.2 Replikation von Backups einrichten

Sie können eine Replikation von Backups konfigurieren, wenn Sie einen Backup-Plan erstellen (S. 58).

- Aktivieren Sie zur Einrichtung einer Replikation, die vom primären Speicherort ausgeht, das Kontrollkästchen **Neu erstelltes Backup zu einem anderen Speicherort replizieren**.
- Aktivieren Sie zur Einrichtung einer Replikation, die vom zweiten oder einen weiteren Speicherort ausgeht, das Kontrollkästchen **Backups, sobald Sie an diesem Speicherort erscheinen, zu einem anderen Speicherort replizieren**.

Bestimmen Sie anschließend den Speicherort, wohin die Backups repliziert werden.

Sofern vom Backup-Schema zugelassen, können Sie zusätzlich festlegen, wann die Backups auf jedem dieser Speicherorte automatisch gelöscht werden sollen.

Ein Backup wird zum jeweils nächsten Speicherort repliziert, sobald es im vorherigen Speicherort erscheint. Falls frühere Backups nicht repliziert wurden (weil beispielsweise die Netzwerkverbindung verloren ging), wird die Software auch alle Backups replizieren, die nach der letzten erfolgreichen Replikation erschienen sind.

4.5.3 Aufbewahrung von Backups einrichten

Aufbewahrungsregeln können bei Erstellung eines Backup-Plans (S. 58) konfiguriert werden. Welche Aufbewahrungsregeln verfügbar sind, hängt vom gewählten Backup-Schema ab.

Das Anwenden von Aufbewahrungsregeln kann durch die Option **Inaktivitätszeit für Replikation/Bereinigung** (S. 110) eingeschränkt werden.

Schema 'Einfach'

Jedes Backup wird solange aufbewahrt, bis sein Alter einen von Ihnen spezifizierten Grenzwert überschreitet. Danach wird es entweder gelöscht oder verschoben.

So konfigurieren Sie, dass die Backups gelöscht werden:

- Wählen Sie in den **Aufbewahrungsregeln** die Option **Lösche Backups älter als...** und spezifizieren Sie dann die Aufbewahrungsdauer.

So konfigurieren Sie, dass die Backups verschoben werden:

- Wählen Sie in den **Aufbewahrungsregeln** die Option **Verschiebe Backups älter als...** und spezifizieren Sie dann die Aufbewahrungsdauer. Spezifizieren Sie unter **Ziel für Replikation/Verschieben der Backups** den entsprechenden Speicherort.

Die Aufbewahrungsregeln werden angewendet, wenn ein Backup erstellt wird. Für den zweiten und weitere Speicherorte bedeutet die Backup-Erstellung, dass ein Backup vom vorherigen Speicherort ausgehend dorthin kopiert oder verschoben wird.

Schema 'Großvater-Vater-Sohn' (GVS)

Backups jeden Typs (täglich, wöchentlich, monatlich) werden für die unter '**Backups behalten**' definierte Aufbewahrungsdauer einbehalten und dann gelöscht.

Die Aufbewahrungsregeln werden angewendet, wenn ein Backup erstellt wird. Sie werden nacheinander auf den primären, sekundären sowie alle nachfolgenden Speicherorte angewendet.

Schema 'Türme von Hanoi'

Jedes Backup wird basierend auf seinem Level (S. 76) einbehalten und dann gelöscht. Wie viele Level das sind, spezifizieren Sie unter **Zahl der Level**.

Die Aufbewahrungsregeln werden angewendet, wenn ein Backup erstellt wird. Sie werden nacheinander auf den primären, sekundären sowie alle nachfolgenden Speicherorte angewendet.

Benutzerdefiniertes Schema

Jedes Backup wird solange aufbewahrt, bis die von Ihnen spezifizierten Regeln zutreffen. Danach wird es entweder gelöscht oder verschoben.

So konfigurieren Sie, dass die Backups gelöscht werden:

- Wählen Sie unter **Archiv bereinigen** die Option **Aufbewahrungsregeln verwenden**. Spezifizieren Sie im Fenster **Aufbewahrungsregeln** (S. 108) die entsprechenden Regeln und wählen Sie dann **Wenn die spezifizierten Bedingungen zutreffen: Die ältesten Backups löschen**.
- Spezifizieren Sie unter **Aufbewahrungsregeln anwenden**, wann die Regeln ausgeführt werden sollen.

So konfigurieren Sie, dass die Backups verschoben werden:

- Wählen Sie unter **Archiv bereinigen** die Option **Aufbewahrungsregeln verwenden**. Spezifizieren Sie im Fenster **Aufbewahrungsregeln** (S. 108) die entsprechenden Regeln und wählen Sie dann **Wenn die spezifizierten Bedingungen zutreffen: Die ältesten Backups an einen anderen Speicherort verschieben**. Klicken Sie auf **OK** und spezifizieren Sie dann unter **Ziel für Replikation/Verschieben der Backups** den entsprechenden Speicherort.
- Spezifizieren Sie unter **Aufbewahrungsregeln anwenden**, wann die Regeln ausgeführt werden sollen.

Sie können wählen, ob die Aufbewahrungsregeln vor der Backup-Erstellung, danach, auf Planung oder gemäß einer Kombination dieser Optionen angewendet werden sollen. Für den zweiten und weitere Speicherorte bedeutet die Backup-Erstellung, dass ein Backup vom vorherigen Speicherort ausgehend dorthin kopiert oder verschoben wird.

4.5.4 Aufbewahrungsregeln für das benutzerdefinierte Schema

Sie können im Fenster **Aufbewahrungsregeln** wählen, wie lange Backups an einem Speicherort vorgehalten werden sollen und ob diese anschließend gelöscht oder verschoben werden sollen.

Die Regeln werden auf alle diejenigen Backups angewendet, die von dieser *speziellen Maschine* gemacht wurden und in diesem *speziellen Speicherort* durch diesen *speziellen Backup-Plan* abgelegt wurden. Ein solcher Satz von Backups wird in Acronis Backup & Recovery 11.5 auch *Archiv* genannt.

So richten Sie Aufbewahrungsregeln für Backups ein:

1. Spezifizieren Sie eine der folgenden Möglichkeiten (Option (a) und (b) schließen sich gegenseitig aus):
   a. **Backups älter als...** und/oder **Archiv größer als...**.

      Ein Backup wird solange gespeichert, bis die spezifizierte Bedingung (oder beide Bedingungen) eintreffen.

      Hinweis: In einem deduplizierenden Depot (S. 488) hat die Bedingung **Archiv größer als** nur einen geringen Einfluss auf den Speicherplatzverbrauch. Der Hintergrund ist, dass nahezu alle Backup-Daten in einem Datenspeicher außerhalb des Archivs gespeichert werden.

      Beispiel:

      Backups älter als 5 Tage

      Archiv größer als 100 GB

      Mit diesen Einstellungen wird ein Backup solange gespeichert, bis es älter als 5 Tage ist *und* die Größe des Archivs, indem es enthalten ist, 100 GB übersteigt.

   b. **Anzahl der Backups im Archiv überschreitet...**

      Fall die Anzahl an Backups den spezifizierten Wert überschreitet, werden eins oder mehrere der ältesten Backups verschoben oder gelöscht. Die kleinste Einstellung ist 1.
2. Bestimmen Sie, ob die Backups gelöscht oder zu einem anderen Speicherort verschoben werden sollen, sofern die angegebenen Bedingungen zutreffen.

Sie können den Speicherort angegeben, zu dem die Backups verschoben werden sollen und nach Klicken auf **OK** auch für diesen Speicherort Aufbewahrungsregeln einstellen.

Das letzte Backup in dem Archiv löschen

Die Aufbewahrungsregeln sind wirksam, wenn das Archiv mehr als ein Backup enthält. Das bedeutet, dass das letzte Backup im Archiv erhalten bleibt, selbst wenn dabei die Verletzung einer Aufbewahrungsregel entdeckt wird. Versuchen Sie nicht, das einzige vorhandene Backup zu löschen, indem Sie die Aufbewahrungsregeln *vor* dem Backup anwenden. Dies wird nicht funktionieren. Verwenden Sie die alternative Einstellung **Archiv bereinigen** –> **Wenn nicht ausreichend Speicherplatz während des Backups vorhanden ist** (S. 74); beachten Sie dabei aber das Risiko, möglicherweise das letzte Backup verlieren zu können.

Backups mit Abhängigkeiten löschen oder verschieben

Klicken Sie zum Zugriff auf diese Einstellungen im Fenster **Aufbewahrungsregeln** auf **Erweiterte Einstellungen anzeigen**.

Aufbewahrungsregeln setzen das Löschen einiger Backups und die Bewahrung anderer voraus. Aber was, wenn das Archiv inkrementelle und differentielle Backups enthält, die voneinander und von dem Voll-Backup abhängen, auf dem diese basieren? Sie können kein veraltetes Voll-Backup löschen und sozusagen seine inkrementellen „Kinder“ behalten.

Wenn das Löschen oder Verschieben eines Backups andere Backups beeinflusst, wird eine der folgenden Regeln angewendet:

- **Backup bewahren, bis alle abhängigen Backups gelöscht (verschoben) werden**

  Das veraltete Backup (mit dem Icon gekennzeichnet) wird solange bewahrt, bis alle auf ihm beruhenden Backups ebenfalls veraltet sind. Dann wird die gesamte Kette während der regulären Bereinigung sofort gelöscht. Falls Sie festgelegt haben, dass die veralteten Backups zum nächsten Speicherort verschoben werden sollen, dann wird das Backup ohne Verzögerung dorthin kopiert. Nur seine Löschung vom aktuellen Speicherort wird aufgeschoben.

  Dieser Modus hilft, die potentiell zeitaufwendige Konsolidierung zu vermeiden, benötigt aber extra Speicherplatz für von der Löschung zurückgestellte Backups. Die Archivgröße, das Backup-Alter oder die Backup-Anzahl kann daher die von Ihnen spezifizierten Werte überschreiten.

  Dieser Modus ist nicht für den Acronis Online Backup Storage verfügbar, wenn Sie Backups dorthin kopieren oder verschieben. Im Online Storage sind alle Backup inkrementell, mit Ausnahme des ersten Backups eines Archivs, welches immer vollständig ist. Diese Kette kann nicht komplett gelöscht werden, weil das aktuellste Backup immer aufbewahrt werden muss.

- **Diese Backups konsolidieren**

  Die Software wird das Backup, das einer Löschung oder Verschiebung unterworfen ist, mit dem nächsten abhängigen Backup konsolidieren. Zum Beispiel erfordern die Aufbewahrungsregeln, ein Voll-Backup zu löschen, das nachfolgende inkrementelle Backup jedoch zu bewahren. Die Backups werden zu einem einzelnen Voll-Backup kombiniert, welches den Zeitstempel des inkrementellen Backups erhält. Wenn ein inkrementelles oder differentielles Backup aus der Mitte einer Kette gelöscht wird, wird der resultierende Backup-Typ inkrementell.

  Dieser Modus stellt sicher, dass nach jeder Bereinigung die Archivgröße, sowie Alter und Anzahl der Backups innerhalb der von Ihnen spezifizierten Grenzen liegen. Die Konsolidierung kann jedoch viel Zeit und Systemressourcen in Anspruch nehmen. Sie benötigen zusätzlichen Platz im Depot für temporäre Daten, die während der Konsolidierung erstellt werden.

  Dieser Modus ist nicht verfügbar, falls Sie die Regel **Archiv größer als** für jeden Archiv-Speicherort (Acronis Online Backup Storage ausgenommen) aktiviert haben.

Das sollten Sie über Konsolidierung wissen

Machen Sie sich bewusst, dass Konsolidierung nur eine Methode, aber keine Alternative zum Löschen ist. Das resultierende Backup wird keine Daten enthalten, die im gelöschten Backup vorlagen, die jedoch im beibehaltenen inkrementellen oder differentiellen Backup fehlten.

4.5.5 Inaktivitätszeit für Replikation/Bereinigung

Diese Option ist nur wirksam, wenn Sie für Backups entweder Replikation oder Aufbewahrungsregeln (S. 104) einrichten.

Die Option definiert einen Zeitraum, in dem der Start einer Replikation oder die Anwendung von Aufbewahrungsregeln nicht erlaubt ist. Diese Aktionen werden daher dann ausgeführt, wenn die Inaktivitätszeit beendet ist und sofern die Maschine zu diesem Zeitpunkt eingeschaltet ist. Aktionen, die vor dem Inaktivitätszeitraum gestartet wurden, werden ohne Unterbrechung fortgesetzt.

Die Inaktivitätszeit betrifft alle Speicherorte, den primären eingeschlossen.

Voreinstellung ist: **Deaktiviert.**

Aktivieren Sie zur Spezifikation der Inaktivitätszeit das Kontrollkästchen **Replikation/Bereinigung in folgender Zeit nicht starten** und wählen Sie dann die Tage und den entsprechenden Zeitraum.

Anwendungsbeispiele

Sie können diese Option auf Wunsch verwenden, um den eigentlichen Backup-Prozess von der Replikation oder Bereinigung zu separieren. Nehmen Sie beispielsweise an, dass Sie Maschinen lokal sowie tagsüber sichern und die entsprechenden Backups dann zu einem Netzwerkordner replizieren. Stellen Sie die Inaktivitätszeit so ein, dass sie die reguläre Arbeitszeit enthält. Die Replikation wird daraufhin nach diesen Arbeitstunden gemacht, wenn auch die Netzwerklast geringer ist.

4.5.6 Anwendungsbeispiele

In diesem Abschnitt finden Sie Beispiele dafür, wie Sie Replikate von Backups erstellen und Aufbewahrungsregeln für diese konfigurieren können.

4.5.6.1 Beispiel 1: Backups zu einem Netzwerkordner replizieren

Betrachten Sie folgendes Szenario:

- Sie möchten Ihre Maschine manuell per Voll-Backup sichern.
- Sie möchten die Backups in der Acronis Secure Zone (S. 217) dieser Maschine speichern.
- Sie möchten eine Kopie der Backups in einem Netzwerkordner speichern.

Erstellen Sie in diesem Szenario einen Backup-Plan mit dem Schema **Manueller Start**. Spezifizieren Sie bei Erstellung des Backup-Plans die Acronis Secure Zone im Feld **Speicherort**, wählen Sie **Vollständig** im Feld **Backup-Typ**, aktivieren Sie das Kontrollkästchen **Neu erstelltes Backup zu einem anderen Speicherort replizieren** – und spezifizieren Sie dann den Netzwerkordner im Feld **2. Speicherort**.

Ergebnis:

- Sie können die Volumes oder Dateien der Maschine von einem sofort verfügbaren, lokalen Backup wiederherstellen, welches in einem speziellen Bereich auf dem Festplattenlaufwerk gespeichert wird.

- Sie können die Maschine aber auch aus dem Netzwerkordner wiederherstellen, falls das Festplattenlaufwerk der Maschine ausfallen sollte.

4.5.6.2 Beispiel 2: Alter und Gesamtgröße gespeicherter Backups begrenzen

Betrachten Sie folgendes Szenario:

- Sie möchten Ihre Maschine mit einem wöchentlichen Voll-Backup sichern.
- Sie möchten alle Backups aufbewahren, die jünger als ein Monat sind.
- Solange die Gesamtgröße aller Backups unterhalb von 200 GB bleibt, möchten Sie zudem auch noch ältere Backups behalten.

Erstellen Sie in diesem Szenario einen Backup-Plan mit dem **Benutzerdefinierten Schema**. Spezifizieren Sie bei Erstellung des Backup-Plans eine wöchentliche Planung für die Voll-Backups. Wählen Sie unter **Archiv bereinigen** die Option **Aufbewahrungsregeln verwenden**.

Klicken Sie auf **Aufbewahrungsregeln**, aktivieren Sie die Kontrollkästchen **Backups älter als** sowie **Archiv größer als** und spezifizieren Sie dann die entsprechenden Werte, nämlich **1 Monat** und **200 GB**. Wählen Sie unter **Wenn die spezifizierten Bedingungen zutreffen** die Einstellung **Älteste Backups löschen**.

Klicken Sie auf **OK**. Aktivieren Sie unter **Aufbewahrungsregeln anwenden** das Kontrollkästchen **Nach dem Backup**.

Ergebnis:

- Backups, die jünger als ein Monat sind, werden aufbewahrt – unabhängig von ihrer Gesamtgröße.
- Backups, die älter als ein Monat sind, werden nur dann aufbewahrt, wenn die Gesamtgröße aller Backups (ältere plus jüngere) nicht die 200 GB-Grenze überschreitet. Anderenfalls löscht die Software einige oder alle der älteren Backups, mit dem ältesten beginnend.

4.5.6.3 Beispiel 3: Replikation von Backups zum Online Storage

Dieses Beispiel geht davon aus, dass Sie ein aktiviertes *(S. 477)* *Online Backup-Abonnement* *(S. 460)* *für die Maschine haben, die Sie per Backup sichern.*

Das folgende Szenario nimmt an, dass die Datenmenge für das Backup relativ klein ist. Informationen zu größeren Backups finden Sie später in diesem Abschnitt unter 'Replikation größerer Datenmengen zum Online Storage'.

Betrachten Sie folgendes Szenario:

- Sie erstellen gelegentliche Backups Ihrer Maschine in einen lokalen Ordner.
- Sie möchten eine Kopie des resultierenden Archivs extern (offsite) im Acronis Online Backup Storage aufbewahren.
- Sie möchten, unabhängig vom Startzeitpunkt des Backups, dass die Replikation außerhalb der üblichen Arbeitszeiten stattfindet, wenn die Belastung der Internetverbindung niedriger ist.

Erstellen Sie in diesem Szenario einen Backup-Plan mit dem gewünschten Backup-Schema. Spezifizieren Sie bei Erstellung des Backup-Plans im Feld **Speicherort** einen lokalen Ordner. Aktivieren Sie das Kontrollkästchen **Neu erstelltes Backup zu einem anderen Speicherort replizieren** und spezifizieren Sie dann im Feld **2. Speicherort** den Online Storage.

Gehen Sie in den **Backup-Optionen** zum Element **Inaktivitätszeit für Replikation/Bereinigung** (S. 110) und spezifizieren Sie die gängigen Arbeitsstunden (beispielsweise Montag bis Freitag von 8:00 bis 17:00 Uhr).

Ergebnis:

- Die Daten werden nach dem Start des Backup-Plans in den lokalen Ordner gesichert.
- Sollte das Backup außerhalb der definierten Arbeitsstunden abgeschlossen werden, dann wird die Replikation sofort gestartet. Anderenfalls wird die Replikation bis zum Ende der Arbeitsstunden verschoben.

Hinweis: *Im Online Storage sind das zweite und alle weiteren Backups eines Archivs immer inkrementell, egal welchen Typ sie am ursprünglichen Speicherort haben. Dadurch wird der Storage-Speicherplatz Ihres Online Backup-Abonnements effizient genutzt.*

Replikation größerer Datenmengen zum Online Storage

Falls Sie planen, Backups mit Daten von 100 GB und mehr zu erstellen, können Sie das erste Backup für den Online Storage auf einer physikalischen Festplatte an uns senden. Diese Option wird Ihnen über den Initial Seeding Service (S. 465) bereitgestellt, den Sie als Ergänzung zu Ihrem Online Backup-Abonnement erwerben können.

Der 'Initial Seeding'-Dienst ist in Ihrer Region möglicherweise nicht verfügbar. Klicken Sie hier für weitere Informationen: http://kb.acronis.com/content/15118.

Bei allen nachfolgenden Backups werden nur noch Änderungen an den ursprünglichen Daten zum Online Storage gesendet, so dass der Netzwerkdatenverkehr nicht zu stark beeinflusst wird.

Erstellen Sie in diesem Szenario einen Backup-Plan mit dem Schema **Initial Seeding**. Spezifizieren Sie bei Erstellung des Backup-Plans im Feld **Speicherort** einen lokalen Ordner. Dies kann ein Ordner auf der zu versendenden Festplatte sein. Weitere Details finden Sie unter 'Wie wird Initial Seeding ausgefьhrt? (S. 466)'.

Bearbeiten Sie den Backup-Plan, nachdem die Festplatte versendet und der Auftragsstatus auf **Der Upload der Daten wurde abgeschlossen** eingestellt wurde. Ändern Sie das Backup-Schema, das Ziel und die Replikationseinstellungen so, wie zuvor in diesem Abschnitt beschrieben.

Der aktualisierte Backup-Plan erstellt Backups, die außerhalb der üblichen Arbeitszeiten zum Online Storage repliziert werden.

4.5.6.4 Beispiel 4: Ältere Backups auf Bänder verschieben

Betrachten Sie folgendes Szenario:

- Sie möchten Ihre Maschine mit einem täglichen Backup sichern.
- Sie möchten diese Backups für eine Woche lokal speichern.
- Backups, die älter als eine Woche sind, sollen auf ein Bandgerät verschoben werden.

Ein solches Szenario wird manchmal auch als 'Disk-Staging' oder D2D2T (Disk-to-Disk-to-Tape) bezeichnet.

Erstellen Sie in diesem Szenario einen Backup-Plan mit dem Schema **Einfach** sowie einer täglichen Planung. (Standardmäßig sind alle Sicherungen Voll-Backups). Spezifizieren Sie bei Erstellung des Backup-Plans im Feld **Speicherort** einen lokalen Ordner oder die Acronis Secure Zone. Wählen Sie unter **Aufbewahrungsregeln** die Einstellung **Verschiebe Backups älter als 1 Woche**. Spezifizieren Sie dann im Feld **2. Speicherort** das Bandgerät.

Stellen Sie sicher, dass das Bandgerät betriebsbereit ist. Die Vorbereitungsschritte sind im Abschnitt 'Backup einer Maschine zu einem direkt angeschlossenen Bandgerдт (S. 228)' beschrieben.

Ergebnis:

- Nach erfolgreichem Abschluss der Sicherung prüft der Agent auf Backups, die verschoben werden müssen.
- Der Agent verschiebt Backups, die älter als eine Woche sind, indem diese zuerst auf das Bandgerät kopiert werden und dann vom ursprünglichen Speicherort gelöscht werden.
- Sie können dann die Bänder mit den Backups auswerfen und an einem sicheren externen Ort aufbewahren. Sobald Sie Daten für eine Wiederherstellung wählen, wird Acronis Backup & Recovery 11.5 Sie nach den einzulegenden Bändern fragen.

4.5.6.5 Beispiel 5: Backup auf Bänder innerhalb eines engen Backup-Fensters

Dieses Beispiel geht davon aus, dass Sie eine Advanced-Edition von Acronis Backup & Recovery 11.5 verwenden.

Betrachten Sie folgendes Szenario:

- Sie möchten Ihre Server an jedem Arbeitstag im Anschluss an die reguläre Arbeitszeit sichern.
- An einem der Arbeitstage möchten Sie ein monatliches Voll-Backup durchführen – an den anderen Werktagen dagegen partielle Backups (inkrementell oder differentiell).
- Sie möchten die Backups auf einer Bandbibliothek speichern.
- Das zeitliche Backup-Fenster für die Server ist eng, so dass sie nicht direkt auf die Bänder gesichert werden können.

Installieren Sie in diesem Szenario den Acronis Backup & Recovery 11.5 Storage Node und erstellen Sie zwei verwaltete Depots: das erste auf einem Festplattenlaufwerk, dass für den Storage Node lokal liegt und das andere auf der Bandbibliothek, die auch lokal an den Storage Node angeschlossen ist.

Erstellen Sie einen zentralen Backup-Plan für alle Maschinen mit dem Schema **Großvater-Vater-Sohn (GVS)**. Spezifizieren Sie bei Erstellung des Backup-Plans im Feld **Speicherort** das Depot auf dem Festplattenlaufwerk. Wählen Sie unter **Backup-Typ** die Einstellung **Vollständig/Inkrementell/Differentiell**.

Wählen Sie für den primären Speicherort unter **Backups behalten** die Einstellung, dass die monatlichen Backups für einen Monat aufbewahrt werden sollen (dazu müssen Sie das Kontrollkästchen **Unbegrenzt behalten** deaktivieren). Auf diese Art dient das Depot als zwischenzeitlicher, kurzfristiger Speicher für die Backups.

Aktivieren Sie das Kontrollkästchen **Neu erstelltes Backup zu einem anderen Speicherort replizieren** und spezifizieren Sie dann im Feld **2. Speicherort** das Depot auf der Bandbibliothek. Wählen Sie für den zweiten Speicherort, dass die monatlichen Backups unbegrenzt aufbewahrt werden sollen.

Ergebnis:

- Die Agenten sichern ihre Maschinen zu dem Depot auf dem Festplattenlaufwerk.
- Der Storage Node kopiert diese Backups dann auf das Bandgerät. Dabei werden keine CPU-Ressourcen von den Maschinen genommen.
- Die Lebenszeit der Backups auf der Festplatte ist nicht höher als einen Monat. Auf der Bandbibliothek werden die monatlichen Backups dagegen unbegrenzt aufbewahrt.

4.6 So deaktivieren Sie die Backup-Katalogisierung

Durch die Katalogisierung eines Backups werden dessen Inhalte direkt nach seiner Erstellung dem Datenkatalog hinzugefügt. Dies kann ein zeitaufwendiges Verfahren sein, insbesondere in Umgebungen mit einer großen Anzahl von Maschinen. Daher möchten Sie möglicherweise die Katalogisierung in der kompletten Umgebung deaktivieren.

So deaktivieren Sie die Backup-Katalogisierung in den Advanced-Editionen

Diese Schritte können in beliebiger Reihenfolge ausgeführt werden.

1. Дndern Sie die Windows-Registry auf dem Management Server.
2. Дndern Sie die Windows-Registry auf den Storage Nodes.
3. [Auf verwalteten Maschinen in einer Active Directory-Domain] Laden Sie das Acronis Administrative Template (S. 444) auf dem Domain-Controller und und konfigurieren Sie die **Katalogisierungseinstellung** in der Template-Kategorie **Acronis Backup & Recovery 11.5 Agent für Windows** (S. 448).
4. [Auf verwalteten Maschinen, die nicht in einer Active Directory-Domain enthalten sind] Verbinden Sie die Konsole mit jeder Maschine, gehen Sie zu **Optionen** –> **Maschinen-Optionen** und konfigurieren Sie die Option **Backup-Katalogisierung**.

4.7 Standardoptionen für Backup

Jeder Acronis Agent hat eigene Standardoptionen für Backups. Sobald ein Agent installiert ist, haben die Standardoptionen vordefinierte Werte, die in der Dokumentation als **Voreinstellungen** bezeichnet werden. Bei Erstellung eines Backup-Plans können Sie entweder eine Standardoption verwenden oder diese mit einem benutzerdefinierten Wert überschreiben, der nur für diesen Plan gültig ist.

Sie können außerdem auch eine Standardoption konfigurieren, indem Sie den vordefinierten Wert verändern. Der neue Wert wird dann als Standard für alle nachfolgend auf dieser Maschine erstellten Backup-Pläne verwendet.

Um die Standardoptionen für Backups einsehen und verändern zu können, verbinden Sie die Konsole mit der verwalteten Maschine und wählen Sie dort aus dem Hauptmenü die Befehle **Optionen** –> **Standardoptionen für Backup und Recovery** –> **Standardoptionen für Backup**.

Verfügbarkeit der Backup-Optionen

Art und Umfang der verfügbaren Backup-Optionen sind abhängig von:

- Der Umgebung, in welcher der Agent arbeitet (Windows, Linux, bootfähiges Medium)
- Dem Datentyp, der gesichert wird (Laufwerke, Dateien).
- Dem Backup-Ziel (Netzwerkpfad oder lokales Laufwerk).
- Dem Backup-Schema (manueller Start oder nach Planung).

Die nachfolgende Tabelle fasst die Verfügbarkeit der Backup-Optionen zusammen:

	Agent für Windows		Agent für Linux		Bootfähiges Medium (Linux-basiert oder PE-basiert)	
	Laufwerk-Backup	**Datei-Backup**	**Laufwerk-Backup**	**Datei-Backup**	**Laufwerk-Backup**	**Datei-Backup**
Erweiterte Einstellungen (S. 117):						
Beim Backup auf ein entfernbares Medium nach dem ersten Medium fragen	Ziel: Wechsel-medium	Ziel: Wechsel-medium	Ziel: Wechsel-medium	Ziel: Wechsel-medium	Ziel: Wechsel-medium	Ziel: Wechsel-medium
Backup nur nach dem Übertragen zum Depot deduplizieren	Ziel: dedupl. Depot	Ziel: dedupl. Depot	Ziel: dedupl. Depot	Ziel: dedupl. Depot	Ziel: dedupl. Depot	Ziel: dedupl. Depot
Archivattribut zurücksetzen	-	+	-	-	-	+
Nach Abschluss des Backups die Maschine automatisch neu starten	-	-	-	-	+	+
Schutz des Archivs (S. 118) (Kennwort und Verschlüsselung)	+	+	+	+	+	+
Backup-Katalogisierung (S. 119)	+	+	+	+	-	-
Backup-Performance:						
Backup-Prioritдt (S. 120)	+	+	+	+	-	-
Schreibgeschwindigkeit auf Laufwerk (S. 121)	Ziel: Laufwerk	Ziel: Laufwerk	Ziel: Laufwerk	Ziel: Laufwerk	Ziel: Laufwerk	Ziel: Laufwerk
Netzwerkverbindungs-geschwindigkeit (S. 121)	Ziel: Netzwerkfrei-gabe	Ziel: Netzwerkfrei-gabe	Ziel: Netzwerkfrei-gabe	Ziel: Netzwerkfrei-gabe	Ziel: Netzwerkfrei-gabe	Ziel: Netzwerkfrei-gabe
Backup-Aufteilung (S. 121)	+	+	+	+	+	+
Komprimierungsgrad (S. 123)	+	+	+	+	+	+
Desaster-Recovery-Plan (S. 123)	+	+	+	+	-	-
Fehlerbehandlung (S. 124):						
Während der Durchführung keine Meldungen bzw. Dialoge zeigen (Stiller Modus)	+	+	+	+	+	+

	Agent für Windows		Agent für Linux		Bootfähiges Medium (Linux-basiert oder PE-basiert)	
	Laufwerk-Backup	Datei-Backup	Laufwerk-Backup	Datei-Backup	Laufwerk-Backup	Datei-Backup
Bei Fehler erneut versuchen	+	+	+	+	+	+
Fehlerhafte Sektoren ignorieren	+	+	+	+	+	+
Ereignisverfolgung:						
Ereignisanzeige von Windows (S. 126)	+	+	-	-	-	-
SNMP (S. 125)	+	+	+	+	-	-
Schnelles inkrementelles/ differentielles Backup (S. 126)	+	-	+	-	+	-
Snapshot fьr Backup auf Dateiebene (S. 127)	-	+	-	+	-	-
Sicherheit auf Dateiebene (S. 127):						
Dateisicherheitsein-stellungen in Archiven bewahren	-	+	-	-	-	-
Verschlüsselte Dateien in Archiven unverschlüsselt speichern	-	+	-	-	-	-
LVM-Snapshot-Erstellung (S. 128)	-	-	+	-	-	-
Medienkomponenten (S. 129)	Ziel: Wechsel-medium	Ziel: Wechsel-medium	Ziel: Wechsel-medium	Ziel: Wechsel-medium	-	-
Mount-Punkte (S. 130)	-	+	-	-	-	-
Multi-Volume-Snapshot (S. 131)	+	+	-	-	-	-
Benachrichtigungen:						
E-Mail (S. 131)	+	+	+	+	-	-
Win Pop-up (S. 133)	+	+	+	+	-	-
Vor-/Nach-Befehle für das Backup (S. 133)	+	+	+	+	nur PE	nur PE
Befehle vor/nach der Datenerfassung (S. 135)	+	+	+	+	-	-
Inaktivitätszeit für Replikation/ Bereinigung (S. 110)	+	+	+	+	-	-

	Agent für Windows		Agent für Linux		Bootfähiges Medium (Linux-basiert oder PE-basiert)	
	Laufwerk-Backup	Datei-Backup	Laufwerk-Backup	Datei-Backup	Laufwerk-Backup	Datei-Backup
Sektor- für -Sektor-Backup (S. 138)	+	-	+	-	+	-
Bandverwaltung (S. 138)	Ziel: Band	Ziel: Band	Ziel: Band	Ziel: Band	Ziel: Band	Ziel: Band
Task-Fehlerbehandlung (S. 140)	+	+	+	+	-	-
Task-Startbedingungen (S. 141)	+	+	+	+	-	-
Volume Shadow Copy Service (S. 142)	+	+	-	-	-	-

4.7.1 Erweiterte Einstellungen

Spezifizieren Sie die zusätzlichen Einstellungen für das Backup durch Aktivieren oder Deaktivieren der folgenden Kontrollkästchen.

Beim Backup auf ein entfernbares Medium nach dem ersten Medium fragen

Diese Option ist nur beim Backup auf Wechselmedien wirksam.

Diese Option definiert, ob die Meldung **Legen Sie das erste Medium ein** erscheint, wenn Sie ein Wechselmedium zum Backup benutzen.

Voreinstellung ist: **Deaktiviert**.

Bei eingeschalteter Option ist es unmöglich, ein Backup auf ein Wechselmedium auszuführen, wenn der Benutzer nicht anwesend ist, weil das Programm auf eine Bestätigung dieser Meldung wartet. Deshalb sollten Sie diese Meldung ausschalten, wenn ein geplanter Task eine Sicherung auf ein Wechselmedium vorsieht. Mit dieser Einstellung kann der Task unbeaufsichtigt erfolgen, wenn ein Wechselmedium beim Start gefunden wird (z.B. eine CD-R/W).

Archivattribut zurücksetzen

Diese Option ist nur für Backups auf Dateiebene unter Windows-Betriebssystemen und beim Arbeiten nach dem Start vom Boot-Medium wirksam.

Voreinstellung ist: **Deaktiviert**.

Im Betriebssystem Windows hat jede Datei ein Attribut **Datei kann archiviert werden**, das über **Datei** –> **Eigenschaften** –> **Allgemein** –> **Erweitert** –> **Archiv- und Indexattribute** verfügbar wird. Dieses Attribut, auch Archiv-Bit genannt, wird durch das Betriebssystem jedes Mal gesetzt, wenn die Datei verändert wurde, und kann durch Backup-Anwendungen zurückgesetzt werden, wenn die Datei in ein Backup auf Dateiebene eingeschlossen wird. Das Archivattribut wird von vielen Anwendungen verwendet, z.B. Datenbanken.

Wenn das Kontrollkästchen **Archivattribut zurücksetzen** aktiviert ist, wird Acronis Backup & Recovery 11.5 das Archivattribut aller im Backup enthaltenen Dateien zurückzusetzen. Acronis Backup &

Recovery 11.5 selbst nutzt das Archiv-Bit aber nicht. Bei Ausführung eines inkrementellen oder differentiellen Backups wird die Änderung einer Datei anhand der Änderung der Dateigröße und von Tag bzw. Zeitpunkt der letzten Speicherung ermittelt.

Nach Abschluss des Backups die Maschine automatisch neu starten

Diese Option ist nur verfügbar, wenn Sie ein Boot-Medium gestartet haben und mit diesem arbeiten.

Voreinstellung ist: **Deaktiviert**.

Wenn die Option eingeschaltet ist, wird Acronis Backup & Recovery 11.5 die Maschine neu starten, nachdem der Backup-Prozess vollendet ist.

Wenn die Maschine standardmäßig z.B. von einer Festplatte bootet und Sie dieses Kontrollkästchen aktivieren, wird unmittelbar nach Abschluss eines Backups durch den bootfähigen Agenten die Maschine neu gestartet werden und das Betriebssystem booten.

Backup nur nach dem Übertragen zum Depot deduplizieren (keine Deduplizierung an der Quelle)

Diese Option ist nur in den Advanced Editions von Acronis Backup & Recovery 11.5 verfügbar.

Diese Option ist für Windows- und Linux-Betriebssysteme und beim Arbeiten nach dem Start vom Boot-Medium wirksam, wenn das Ziel des Backups ein deduplizierendes Depot ist.

Voreinstellung ist: **Deaktiviert**.

Das Aktivieren dieser Option schaltet die Deduplizierung der Backups an der Quelle aus, d.h. die Deduplizierung erfolgt durch den Acronis Backup & Recovery 11.5 Storage Node, nachdem das Backup im Depot abgelegt ist (auch Deduplizierung am Ziel genannt).

Das Abschalten der Deduplizierung an der Quelle führt zu einem schnelleren Backup-Prozess, aber auch zu größerem Datenverkehr über das Netzwerk und schwererer Last auf dem Storage Node. Die resultierende Größe des Backups im Depot ist unabhängig davon, ob die Deduplizierung an der Quelle eingeschaltet ist oder nicht.

Die Funktionen 'Deduplizierung an der Quelle' und 'Deduplizierung am Ziel' sind beschrieben unter Deduplizierung – ьberblick (S. 259).

4.7.2 Schutz des Archivs

Diese Option ist für Windows-, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Option ist wirksam für Disk-Backups und Backups auf Dateiebene.

Diese Option definiert, ob das Archiv per Kennwort geschützt und der Inhalt des Archivs verschlüsselt werden soll.

Diese Option ist nicht verfügbar, wenn das Archiv bereits Backups enthält. Diese Option kann beispielsweise nicht verfügbar sein:

- Wenn Sie ein bereits existierendes Archiv als Ziel für einen Backup-Plan spezifizieren.
- Wenn Sie einen Backup-Plan bearbeiten, der bereits zu einem Backup geführt hat.

Voreinstellung ist: **Deaktiviert.**

So schützen Sie ein Archiv vor unberechtigtem Zugriff

1. Aktivieren Sie das Kontrollkästchen **Kennwort für das Archiv einrichten**.
2. Tragen Sie im Eingabefeld **Kennwort** ein Kennwort ein.
3. Tragen Sie das Kennwort im Eingabefeld **Kennwortbestätigung** erneut ein.
4. Wählen Sie eine der nachfolgenden Varianten:
   - **Nicht verschlüsseln** – das Archiv wird nur mit dem Kennwort geschützt.
   - **AES 128** – das Archiv wird mit Hilfe des Advanced Encryption Standard-Verfahrens (AES) und einer Tiefe von 128-Bit verschlüsselt.
   - **AES 192** – das Archiv wird mit Hilfe von Advanced Standard Encryption (AES) und einer Tiefe von 192-Bit verschlüsselt.
   - **AES 256** – das Archiv wird mit Hilfe von Advanced Standard Encryption (AES) und einer Tiefe von 256-Bit verschlüsselt.
5. Klicken Sie auf **OK**.

Der kryptografische Algorithmus AES arbeitet im Cipher Block Chaining Mode (CBC) und benutzt einen zufällig erstellten Schlüssel mit der benutzerdefinierten Größe von 128-, 192- oder 256-Bit. Je größer die Schlüsselgröße, desto länger wird das Programm für die Verschlüsselung brauchen, aber desto sicherer sind auch die Daten.

Der Kodierungsschlüssel ist dann mit AES-256 verschlüsselt, wobei ein SHA-256-Hash-Wert des Kennworts als Schlüssel dient. Das Kennwort selbst wird nirgendwo auf dem Laufwerk oder in der Backup-Datei gespeichert, der Kennwort-Hash dient nur der Verifikation. Mit dieser zweistufigen Methode sind die gesicherten Daten vor unberechtigten Zugriff geschützt – ein verlorenes Kennwort kann daher jedoch auch nicht wiederhergestellt werden.

4.7.3 Backup-Katalogisierung

Beim Katalogisieren eines Backups werden dessen Inhalte zum Datenkatalog hinzugefügt. Durch Verwendung des Datenkatalogs können Sie benötigte Daten leicht finden und für eine Recovery-Aktion auswählen.

Die Option **Backup-Katalogisierung** spezifiziert, ob mit dem Backup direkt nach seiner Erstellung eine vollständige oder schnelle Katalogisierung durchgeführt wird.

Diese Option ist nur wirksam, falls die Backup-Katalogisierung auf der gesicherten Maschine oder auf dem Storage Node aktiviert ist.

Voreinstellung ist: **Vollständige Katalogisierung.**

Falls Sie **Vollständige Katalogisierung** wählen, werden die Backup-Inhalt mit dem höchstmöglichen Detail-Level katalogisiert. Das bedeutet, dass folgende Daten im Katalog angezeigt werden:

- Bei Laufwerk-Backups – Laufwerke, Volumes, Dateien und Ordner.
- Bei Datei-basierten Backups – Dateien und Ordner.
- Bei einem Exchange-Datenbank-Backup – Datenbanken oder Speichergruppen und Postfächer (immer); Ordner und E-Mails (abhängig von der Option **Microsoft Exchange-Metadatensammlung**).
- Bei einem Exchange-Postfach-Backup – Postfächer, Ordner und E-Mails.

Sie können die **Schnelle Katalogisierung** wählen, falls die vollständige Katalogisierung die Performance der verwalteten Maschine zu stark beeinflusst oder das Fenster für die Backup-Erstellung zu eng ist. Folgende Daten werden im Katalog angezeigt:

- Bei Laufwerk-Backups – nur Laufwerke und Volumes.
- Bei Datei-basierten Backups – nichts.
- Bei einem Exchange-Datenbank-Backup – nur Datenbanken oder Speichergruppen und Postfächer.
- Bei einem Exchange-Postfach-Backup – nur Postfächer.

Um dem Katalog die vollständigen Inhalte bereits existierender Backups hinzuzufügen, können Sie die vollständige Katalogisierung bei Bedarf auch manuell starten.

Hinweis für Benutzer der Virtual Edition: *Beim Backup zu einem unverwalteten Depot (ausgenommen bei einem lokal angeschlossenen Storage), führt der Agent für ESX(i) (Virtuelle Appliance) immer eine* ***schnelle Katalogisierung*** *durch. Sie können die vollständige Katalogisierung des Depots manuell vom Management Server aus starten.*

Weitere Informationen zur Verwendung dieser Funktion finden Sie im Abschnitt 'Datenkatalog (S. 150)'.

4.7.4 Backup-Performance

Benutzen Sie diese Gruppe der Optionen, um die Nutzung der Netzwerk- und der System-Ressourcen zu steuern.

Die Optionen zur Steuerung der Performance haben mehr oder weniger spürbare Auswirkungen auf die Geschwindigkeit des Backups. Die Wirkung hängt von den Systemkonfigurationen und den physikalischen Eigenschaften der Geräte ab, die beim Backup als Quelle oder Ziel benutzt werden.

4.7.4.1 Backup-Priorität

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Beinhaltet ein Backup-Plan eine Validierung und ist das Backup-Ziel zudem kein verwaltetes Depot, dann ist diese Option für Backups und Validierungen gleichermaßen wirksam.

Die Priorität eines jeden Prozesses, der in einem System läuft, hängt vom Grad der CPU-Benutzung und der Systemressourcen ab, die dem Prozess zugeordnet werden. Das Herabsetzen der Backup-Priorität wird mehr Ressourcen für andere Anwendungen freisetzen. Das Heraufsetzen der Backup-Priorität kann den Backup-Prozess beschleunigen, indem z.B. CPU-Ressourcen von anderen gleichzeitig laufenden Prozessen abgezogen werden. Der Effekt ist aber abhängig von der totalen CPU-Auslastung und anderen Faktoren wie der Schreibgeschwindigkeit der Festplatte oder dem Datenverkehr im Netzwerk.

Voreinstellung ist: **Niedrig.**

So spezifizieren Sie die Priorität des Backup-Prozesses

Wählen Sie eine der nachfolgenden Varianten:

- **Niedrig** – minimiert die durch den Backup-Prozess verwendeten Ressourcen und belässt mehr Ressourcen für andere Prozesse, die auf der Maschine laufen.
- **Normal** – führt den Backup-Prozess mit normaler Geschwindigkeit aus und teilt die verfügbaren Ressourcen mit anderen Prozessen.
- **Hoch** – maximiert die Geschwindigkeit des Backup-Prozesses und zieht Ressourcen von anderen Prozessen ab.

4.7.4.2 Schreibgeschwindigkeit der Festplatte

Diese Option ist für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Option steht zur Verfügung, wenn eine interne (feste) Festplatte der Maschine als Backup-Ziel für das laufende Backup gewählt wurde.

Ein laufendes Backup auf einer internen Festplatte (z.B. in der Acronis Secure Zone) kann die Performance anderer Programme beeinträchtigen, weil eine große Datenmenge auf die Festplatte geschrieben werden muss. Sie können den Festplattengebrauch durch das Backup-Verfahren auf einen gewünschten Grad begrenzen.

Voreinstellung ist: **Maximum.**

So stellen Sie die gewünschte Schreibgeschwindigkeit für das Backup ein

Wählen Sie aus den nachfolgenden Varianten:

- Klicken Sie auf **Schreibgeschwindigkeit in Prozent bezogen auf die maximale Geschwindigkeit der Zielfestplatte** und verändern Sie dann mit dem Schieber den Prozentwert.
- Klicken Sie auf **Schreibgeschwindigkeit in Kilobytes pro Sekunde** und tragen Sie dann den gewünschten Wert in Kilobytes pro Sekunde ein.

4.7.4.3 Netzwerkverbindungsgeschwindigkeit

Diese Option ist für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Option steht zur Verfügung, wenn ein Speicherort im Netzwerk (freigegebenes Netzlaufwerk, verwaltetes Depot oder FTP-/SFTP-Server) als Ziel für das Backup gewählt wurde.

Beinhaltet ein Backup-Plan eine Validierung und ist das Backup-Ziel zudem kein verwaltetes Depot, dann ist diese Option für Backups und Validierungen gleichermaßen wirksam.

Die Option definiert den Betrag der Bandbreite für die Netzwerkverbindung, die zum Übertragen der gesicherten Daten zugeteilt wird.

Als Standard ist dieser Wert auf das Maximum gesetzt, d.h. die Software benutzt die gesamte Netzwerkbandbreite zum Übertragen der gesicherten Daten, die sie erhalten kann. Verwenden Sie diese Option, um einen Teil der Netzwerkbandbreite für andere Aktivitäten im Netzwerk zu reservieren.

Voreinstellung ist: **Maximum.**

So stellen Sie die Netzwerkverbindungsgeschwindigkeit ein

Wählen Sie aus den nachfolgenden Varianten:

- Klicken Sie auf **Datendurchsatz in Prozent bezogen auf die geschätzte maximale Netzwerkverbindungsgeschwindigkeit** und verändern Sie dann mit dem Schieber den Prozentwert.
- Klicken Sie auf **Datendurchsatz in Kilobytes pro Sekunde** und tragen Sie dann den gewünschten Wert in Kilobytes pro Sekunde ein.

4.7.5 Backup-Aufteilung

Diese Option ist für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Option ist nicht wirksam, wenn das Backup-Ziel ein verwaltetes Depot oder der Acronis Online Backup Storage ist.

Die Option definiert, wie ein Backup aufgeteilt werden kann.

Voreinstellung ist: **Automatisch**

Es stehen die folgenden Einstellungen zur Verfügung.

Automatisch

Mit dieser Einstellung wird Acronis Backup & Recovery 11.5 wie folgt arbeiten.

- **Bei Backups zu einem Festplattenlaufwerk oder eine Netzwerkfreigabe:**

  Es wird eine einzige Backup-Datei erstellt werden, wenn das Dateisystem des Ziels die geschätzte Dateigröße erlaubt.

  Das Backup wird automatisch in mehrere Dateien aufgeteilt, wenn das Dateisystem des Ziels die geschätzte Dateigröße erlaubt. Das ist beispielsweise der Fall, wenn das Backup in einem FAT16- oder FAT32-Dateisystem mit einer Dateigrößenbeschränkung von 4 GB abgelegt wird.

  Wenn das Ziellaufwerk während des Backups voll läuft, wechselt der Task in den Zustand **Benutzereingriff erforderlich**. Sie haben dann die Möglichkeit, zusätzlichen Speicherplatz frei zu machen und die Aktion zu wiederholen. In diesem Fall wird das resultierende Backup in zwei Teile gesplittet, die vor bzw. nach der Wiederholung erstellt wurden.

- **Beim Backup auf Wechselmedien** (CD, DVD, Blu-Ray Disc, einem autonomen Bandlaufwerk, einem RDX- oder USB-Laufwerk im Wechsellaufwerksmodus (S. 221)):

  Der Task wird in den Status **Benutzereingriff erforderlich** wechseln und nach einem neuen Medium fragen, wenn das vorhergehende voll ist.

- **Beim Backup auf einen FTP-Server:**

  Das Backup wird automatisch in Dateien von maximal 2 GB aufgeteilt. Die Aufteilung ist notwendig, damit eine Datenwiederherstellung direkt vom FTP-Server möglich ist.

- **Beim Backup auf einen SFTP-Server:**

  Eine einzelne Backup-Datei wird erstellt. Wenn der als Ziel verwendete Storage während des Backups voll läuft, schlägt der Task fehl.

Wenn Sie ein Backup replizieren oder verschieben (S. 104) (zu einem anderen Speicherort), dann gelten diese Regeln für jeden Speicherort unabhängig.

Beispiel:
Angenommen, dass der primäre Speicherort für ein 3-GB-Backup eine Festplatte ist, der zweite Speicherort ein FTP-Server und der dritte eine Netzwerkfreigabe. In diesem Fall wird das Backup in Form einer einzelnen Datei im primären Speicherort hinterlegt, in Form von zwei Dateien im zweiten Speicherort und wiederum als eine einzelne Datei im dritten Speicherort.

Feste Größe

Tragen Sie die gewünschte Dateigröße ein oder wählen Sie diese aus dem Listenfeld. Das Backup wird in mehrere Dateien der angegebenen Größe aufgeteilt. Das ist praktisch, wenn Sie ein Backup mit der Absicht erstellen, dieses nachträglich auf eine CD oder DVD zu brennen. Sie können ein Backup auch selbst in 2 GB große Dateien aufteilen, falls Sie die Sicherung zuerst auf ein Festplattenlaufwerk durchführen und planen, das Backup später manuell auf einen FTP-Server zu kopieren.

4.7.6 Komprimierungsrate

Diese Option ist für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Die Option definiert den Grad der Komprimierung für die zu sichernden Daten.

Voreinstellung ist: **Normal.**

Der ideale Grad für die Datenkomprimierung hängt von der Art der Daten ab, die gesichert werden sollen. So wird z.B. eine maximale Komprimierung die Größe einer Archivdatei nicht wesentlich beeinflussen, wenn bereits stark komprimierte Dateien im Archiv erfasst werden wie jpg-, pdf- oder mp3-Dateien. Andere Typen, wie z.B. doc- oder xls-Dateien, werden gut komprimiert.

So spezifizieren Sie den Komprimierungsgrad

Wählen Sie eine der nachfolgenden Varianten:

- **Keine** – die Daten werden so gesichert, wie sie sind, ohne dabei komprimiert zu werden. Die entstehende Größe des Backup-Archivs wird maximal sein.
- **Normal** – in den meisten Fällen empfohlen.
- **Hoch** – die Größe des entstehenden Backups ist üblicherweise kleiner als die bei der Einstellung **Normal**.
- **Maximum** – die Daten werden so sehr komprimiert, wie es geht. Die Dauer eines solchen Backups wird maximal sein. Sie könnten beim Backup auf Wechselmedien die maximale Komprimierung auswählen, um die Zahl der erforderlichen Medien zu verringern.

4.7.7 Desaster-Recovery-Plan (DRP)

Diese Option ist für Windows und Linux wirksam, aber nicht für Boot-Medium anwendbar.

Diese Option ist nicht für Datei-Backups wirksam.

Ein Desaster-Recovery-Plan (DRP) enthält eine Liste per Backup gesicherter Datenelemente sowie genaue Anweisungen, mit denen ein Benutzer durch den Prozess geführt wird, diese Elemente von einem Backup wiederherstellen zu können.

Ein DRP wird erstellt, sobald das erste Backup erfolgreich vom Backup-Plan durchgeführt wurde. Falls die Option **Desaster-Recovery-Pläne senden** aktiviert ist, wird der DRP per E-Mail an die spezifizierte Liste der Benutzer versendet. Falls die Option **DRP als Datei speichern** aktiviert ist, wird der DRP als Datei an dem spezifizierten Speicherort hinterlegt. Der DRP wird außerdem erneut in folgenden Fällen erstellt:

- Der Backup-Plan wurde bearbeitet, so dass sich die DRP-Parameter geändert haben.
- Das Backup enthält neue Datenelemente oder zuvor gesicherte Elemente sind nicht mehr enthalten. (Gilt nicht für Datenelemente wie Dateien oder Ordner.)

Falls mehrere Maschinen durch einen Backup-Plan geschützt werden, dann wird ein separater DRP für jede Maschine erstellt. Sie können einen lokalen Ordner (bei direkter Verbindung mit einer verwalteten Maschine), einen Netzwerkordner, einen FTP- oder SFTP-Server als Ort zum Speichern der DRPs spezifizieren.

DRP und 'Nach'-Befehle für das Backup

Beachten Sie, dass der DRP nicht automatisch geändert wird, falls 'Nach'-Backup-Befehle Ihres Backup-Plans die Backups vom ursprünglichen Speicherort aus kopieren oder verschieben. Der DRP verweist nur auf die im Backup-Plan spezifizierten Speicherorte.

Einer DRP-Vorlage Informationen hinzufügen

Falls Sie mit XML und HTML vertraut sind, können Sie einer DRP-Vorlage (Template) zusätzliche Informationen hinzufügen. Die Standard-Pfade zur DRP-Vorlage sind:

- **%ProgramFiles%\Acronis\BackupAndRecovery\drp.xsl** – in einem 32 Bit Windows
- **%ProgramFiles(x86)%\Acronis\BackupAndRecovery\drp.xsl** – in einem 64 Bit Windows
- **/usr/lib/Acronis/BackupAndRecovery/drp.xsl** – in Linux

So konfigurieren Sie das Versenden von DRPs:

1. Aktivieren Sie das Kontrollkästchen **Desaster-Recovery-Pläne senden**.
2. Geben Sie die E-Mail-Adresse in das Eingabefeld **E-Mail-Adresse** ein. Sie können mehrere E-Mail-Adressen nacheinander eintragen, je durch Semikolon getrennt.
3. [Optional] Ändern Sie, falls erforderlich, das Feld **Betreff**.

   Falls Sie mehrere Maschinen mit einem zentralen Backup-Plan sichern und wollen, dass jeder Maschinenbenutzer eine separate DRP-E-Mail nur für seine Maschine erhält:

   a. Verwenden Sie die Variable *%MachineName%* , damit der Name der entsprechenden Maschine in der E-Mail-Betreffzeile angezeigt wird.
   b. Konfigurieren Sie Ihren Mail-Server oder die Clients so, dass E-Mails auf Basis des Feldes **Betreff** gefiltert bzw. weitergeleitet werden.
4. Geben Sie die Parameter zum Zugriff auf den SMTP-Server ein. Zu weiteren Informationen siehe E-Mail-Benachrichtigungen (S. 185).
5. [Optional] Klicken Sie auf **Test-Mail senden**, um die Richtigkeit der Einstellungen zu überprüfen.

So konfigurieren Sie das Speichern der DRPs als Dateien:

1. Aktivieren Sie das Kontrollkästchen **DRP als Datei speichern**.
2. Klicken Sie auf **Durchsuchen**, um einen Speicherort für die DRP-Dateien zu spezifizieren.

4.7.8 Fehlerbehandlung

Diese Optionen sind für Windows- und Linux-Betriebssysteme sowie Boot-Medien wirksam.

Mit diesen Optionen können Sie festlegen, wie eventuell auftretende Fehler beim Backup behandelt werden.

Während der Durchführung keine Meldungen bzw. Dialoge zeigen (Stiller Modus)

Voreinstellung ist: **Deaktiviert**.

Wenn der stille Modus eingeschaltet ist, kann das Programm Situationen automatisch behandeln, die eine Benutzeraktion erfordern (außer der Behandlung von fehlerhaften Sektoren, die mit einer eigenen Option gesteuert wird). Falls eine Aktion nicht ohne Benutzereingriff fortfahren kann, wird sie fehlschlagen. Detaillierte Informationen über die Aktion, einschließlich eventueller Fehler, finden Sie im Log der Aktion.

Bei Fehler erneut versuchen

Voreinstellung ist: **Aktiviert. Anzahl der Versuche: 30. Abstand zwischen den Versuchen: 30 Sekunden.**

Wenn ein behebbarer Fehler auftritt, versucht das Programm, die erfolglose Aktion erneut durchzuführen. Sie können das Zeitintervall und die Anzahl der Versuche einstellen. Die Versuche werden aufgegeben, wenn entweder die Aktion erfolgreich ist ODER die angegebene Anzahl an Versuchen erreicht wurde, je nachdem, was zuerst eintritt.

Wenn der Speicherort des Backups im Netzwerk nicht verfügbar oder erreichbar ist, wird die Anwendung versuchen, den Ort alle 30 Sekunden erneut zu erreichen, aber nur fünf Mal. Die Versuche werden aufgegeben, wenn entweder die Verbindung gelingt ODER die angegebene Zahl der Versuche erreicht ist, je nachdem, was zuerst eintritt.

Sollte der Acronis Online Backup Storage als erster, zweiter oder ein weiterer Backup-Speicherort ausgewählt sein, dann lautet die automatische Einstellung des Optionswerts ***Aktiviert. Anzahl der Versuche: 300****, unabhängig vom Standardwert.*

Fehlerhafte Sektoren ignorieren

Voreinstellung ist: **Deaktiviert**.

Wenn die Option unwirksam gemacht ist, wird das Programm jedes Mal ein Pop-up-Fenster zeigen, wenn es auf einen fehlerhaften Sektor stößt, und um eine Entscheidung bitten, ob das Backup fortgesetzt oder abgebrochen werden soll. Wenn Sie z.B. vorhaben, die Informationen von einer 'sterbenden' Festplatte zu retten, aktivieren Sie diese Funktion. Die restlichen Daten werden in diesem Fall noch gesichert und Sie werden das entstandene Laufwerk-Backup mounten und die noch gültigen Daten auf ein anderes Laufwerk kopieren können.

4.7.9 Ereignisverfolgung

Es ist möglich, die von den Backup-Aktionen auf verwalteten Maschinen erstellten Logs in die Ereignisanzeige von Windows zu duplizieren oder an spezifizierte SNMP-Manager zu senden.

4.7.9.1 SNMP-Benachrichtigungen

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Diese Option definiert, ob Agenten auf verwalteten Maschinen Log-Ereignisse von Backup-Aktionen zu spezifizierten Simple Network Management Protocol (SNMP)-Managern schicken. Sie können die Arten der Ereignisse wählen, die geschickt werden.

Zu weiteren Informationen über die Verwendung von SNMP mit Acronis Backup & Recovery 11.5 siehe „Unterstьtzung fьr SNMP (S. 56)“.

Voreinstellung ist: **Einstellungen benutzen, die in den Optionen für die Maschine definiert sind.**

So wählen Sie, ob Ereignisse von Backup-Aktionen an SNMP-Manager geschickt werden:

Wählen Sie eine der folgenden Optionen:

- **Einstellungen benutzen, die in den Optionen für die Maschine definiert sind** – für die Benutzung der Einstellungen, die in den Optionen für die Maschine spezifiziert sind. Weitere Informationen bei Optionen der Maschine.
- **SNMP-Benachrichtigungen für Ereignisse bei Backup-Aktionen einzeln senden** – für das Senden von SNMP-Benachrichtigungen mit den Ereignissen bei Backup-Aktionen an spezifizierte SNMP-Manager.
  - **Ereignisse, die übermittelt werden** – Auswahl der Ereignistypen, die gesendet werden: **Alle Ereignisse**, **Fehler und Warnungen** oder **Nur Fehler**.
  - **Server-Name/IP** – Eintragen des Namens oder der IP-Adresse des Hosts mit der SNMP-Verwaltungsanwendung, an die die Meldungen gesendet werden.

    - **Community** – Eintragen des Namens der SNMP-Community, zu der der Host mit der SNMP-Verwaltungsanwendung und die sendende Maschine gehören. Die typische Community ist „public“.

  Klicken Sie auf **Testnachricht senden**, um die Richtigkeit der Einstellungen zu prüfen.

- **Keine SNMP-Benachrichtigungen senden** – Einstellung, um das Versenden von Ereignissen über Backup-Aktionen an SNMP-Manager unwirksam zu machen.

4.7.9.2 Ereignisanzeige von Windows

Diese Option ist nur wirksam in Windows-Betriebssystemen.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Diese Option definiert, ob Agenten auf verwalteten Maschinen die Ereignisse der Backup-Aktionen in der Ereignisanzeige von Windows aufzeichnen müssen. (Um die Ereignisanzeige zu sehen, führen Sie **eventvwr.exe** aus oder den Befehl **Systemsteuerung -> Verwaltung -> Ereignisanzeige**.) Sie können die Ereignisse filtern, die geloggt werden.

Voreinstellung ist: **Einstellungen benutzen, die in den Optionen für die Maschine definiert sind.**

Wählen Sie, ob Ereigniseinträge der Backup-Aktionen an die Ereignisanzeige von Windows übergeben werden.

Wählen Sie eine der folgenden Optionen:

- **Einstellungen benutzen, die in den Optionen für die Maschine definiert sind** – für die Benutzung der Einstellungen, die in den Optionen für die Maschine spezifiziert sind. Weitere Informationen bei Optionen der Maschine.
- **Folgende Ereignisse protokollieren** – für das Loggen der Ereignisse der Backup-Aktionen in der Ereignisanzeige. Arten der Ereignisse, die geloggt werden:
    - **Alle Ereignisse** – loggt alle Ereignisse (Informationen, Warnungen und Fehler)
    - **Fehler und Warnungen**
    - **Nur Fehler**
- **Nicht protokollieren** – für das Ausschalten der Protokollierung der Ereignisse der Backup-Aktionen in der Ereignisanzeige.

4.7.10 Beschleunigtes inkrementelles und differentielles Backup

Diese Option ist für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Option ist wirksam für inkrementelle und differentielle Backups auf Dateiebene.

Diese Option definiert, ob für die Ermittlung einer Dateiänderung die Dateigröße und der Zeitstempel benutzt werden oder dafür der Dateiinhalt mit den im Archiv gespeicherten Dateien verglichen wird.

Voreinstellung ist: **Aktiviert.**

Inkrementelle oder differentielle Backups erfassen nur die geänderten Daten. Um das Backup-Verfahren zu beschleunigen, entscheidet das Programm darüber, ob eine Datei geändert wurde oder nicht, anhand von Dateigröße und Zeitstempel der letzten Änderung. Das Ausschalten dieser Funktion wird dazu führen, dass das Programm immer den Inhalt einer Datei mit dem Inhalt der Datei vergleicht, die in einem Archiv gespeichert ist.

4.7.11 Snapshot für Backup auf Dateiebene

Diese Option ist nur für Backups auf Dateiebene wirksam in Windows- und Linux-Betriebssystemen.

Diese Option definiert, ob Dateien eine nach der anderen gesichert werden oder auf Basis eines sofortigen Snapshots der Daten.

Beachten Sie: *Dateien von Netzlaufwerken werden immer eine nach der anderen gesichert.*

Voreinstellung ist: **Snapshot erstellen, wenn es möglich ist.**

Wählen Sie eine der nachfolgenden Varianten:

- **Immer einen Snapshot erstellen**

  Ein Snapshot ermöglicht das Backup aller Dateien einschließlich solcher, die für den exklusiven Zugriff geöffnet sind. Die Dateien werden zum gleichen Zeitpunkt gesichert. Wählen Sie diese Einstellung nur, wenn diese Faktoren kritisch sind, d.h. ein Backup der Dateien ohne den vorhergehenden Snapshot keinen Sinn macht. Um einen Snapshot zu benutzen, muss der Backup-Plan mit einem Administrator-Konto oder den Rechten eines Backup-Operators ausgeführt werden. Wenn kein Snapshot erstellt werden kann, wird das Backup fehlschlagen.

- **Snapshot erstellen, wenn es möglich ist**

  Dateien direkt sichern, wenn kein Snapshot möglich ist.

- **Keinen Snapshot erstellen**

  Dateien immer direkt sichern. Administratorrechte oder Rechte eines Backup-Operators sind nicht erforderlich. Der Versuch zum Sichern von Dateien, die für exklusiven Zugriff geöffnet sind, wird in einem Fehler resultieren. Außerdem ist die Backup-Zeit der Dateien nicht gleich.

4.7.12 Sicherheit auf Dateiebene

Diese Optionen sind nur für Backups auf Dateiebene unter Windows-Betriebssystemen wirksam.

Verschlüsselte Dateien in Archiven unverschlüsselt speichern

Diese Option definiert, ob die Dateien vor der Speicherung im Archiv entschlüsselt werden.

Voreinstellung ist: **Ausgeschaltet**.

Ignorieren Sie diese Option, wenn Sie keine Verschlüsselung benutzen. Aktivieren Sie diese Option, wenn verschlüsselte Dateien in das Backup einbezogen werden und Sie wollen, dass ein beliebiger Benutzer nach der Wiederherstellung auf die Dateien zugreifen kann. Andernfalls wird nur der Benutzer, der die Dateien bzw. Verzeichnisse ursprünglich verschlüsselt hat, darauf zugreifen können. Die Entschlüsselung ist auch nützlich, wenn Sie verschlüsselte Dateien auf verschiedenen Maschinen wiederherstellen wollen.

Die Dateiverschlüsselung steht in Windows zur Verfügung unter Verwendung des NTFS-Dateisystems mit Encrypting File System (EFS). Um auf die Verschlüsselungseinstellungen einer Datei oder eines Verzeichnisses zuzugreifen, wählen Sie ***Eigenschaften > Allgemein > Erweitert> Inhalt verschlüsseln****.*

Dateisicherheitseinstellungen in Archiven erhalten

Diese Option definiert, ob die NTFS-Zugriffsrechte für Dateien zusammen mit den Dateien gesichert werden.

Voreinstellung ist: **Aktiviert.**

Wenn die Option eingeschaltet ist, werden Dateien und Ordner mit der ursprünglichen Erlaubnis zum Lesen, Schreiben oder Ausführen für jeden Benutzer oder jede Benutzergruppe im Archiv gespeichert. Wenn Sie auf einer Maschine geschützte Dateien bzw. Ordner ohne den in den Berechtigungen angegebenen Benutzer wiederherstellen, werden Sie wahrscheinlich nicht in der Lage sein, diese Dateien bzw. Ordner zu lesen oder zu verändern.

Um dieses Problem zu beseitigen, sollten Sie die Aufbewahrung von Dateisicherheitseinstellungen in Archiven unwirksam machen. Die wiederhergestellten Dateien und Ordner erben dann immer die Rechte des Ordners, in den sie wiederhergestellt werden, oder die der Festplatte, wenn sie an der Wurzel wiederhergestellt werden.

Alternativ können Sie die Wiederherstellung (S. 184) der Sicherheitseinstellungen unwirksam machen, selbst wenn diese im Archiv gespeichert sind. Das Ergebnis wird das gleiche sein – die Dateien erben die Zugriffsrechte vom übergeordneten Ordner.

Um auf die NTFS-Zugriffsrechte von Datei oder Ordnern zuzugreifen, wählen Sie ***Eigenschaften*** *>* ***Sicherheit****>.*

4.7.13 LVM-Snapshot-Erstellung

Diese Option ist nur für Linux-Betriebssysteme wirksam. Diese Option ist für Laufwerk- und Datei-Backups von Volumes wirksam, die vom Linux Logical Volume Manager (LVM) verwaltet werden. Solche Volumes werden auch als 'logische Volumes' bezeichnet.

Diese Option definiert, wie der Snapshot eines logischen Volumes erfasst wird. Acronis Backup & Recovery 11.5 kann dies eigenständig tun oder den Linux Logical Volume Manager (LVM) beanspruchen. Die Verwendung von Snapshots gewährleistet, dass von einem Volume, dessen Daten sich möglicherweise während des Backup-Prozesses verändern, ein zeitkonsistentes Backup erstellt wird.

Voreinstellung ist: **Acronis Backup & Recovery 11.5**

Wählen Sie eine der nachfolgenden Varianten:

- **Acronis Backup & Recovery 11.5**

Acronis Backup & Recovery 11.5 wird den Snapshot eigenständig erfassen. Mit dieser Einstellung erfolgt das Backup normalerweise schneller und es ist kein 'nicht zugeordneter' Speicherplatz auf der Volume-Gruppe erforderlich. Wir empfehlen die Voreinstellung daher nur zu ändern, falls es ansonsten zu Problemen beim Backup von logischen Volumes kommt.

- **Logical Volume Manager**

Acronis Backup & Recovery 11.5 wird das durch den LVM erfasste Snapshot verwenden. Dieser Snapshot wird auf 'nicht zugeordnetem' Speicherplatz der Volume-Gruppe gespeichert. Falls es keinen 'nicht zugeordneten' Speicherplatz gibt, wird Acronis Backup & Recovery 11.5 den Snapshot eigenständig erfassen.

Detaillierte Erläuterung der LVM-Snapshot-Erfassung

Wenn ein Volume-Snapshot erfasst wurde und die Daten sich zu ändern beginnen, müssen die alten Daten irgendwo aufbewahrt werden, bis sie in das Backup gesichert wurden.

- Acronis behält die alten Daten größtenteils im RAM. (Während eines Datei-Backups erstellt die Software evtl. eine temporäre Datei unter **/tmp**, falls die Größe der alten Daten erheblich wächst.)
- LVM benötigt ein temporäres logisches Volume (ein logisches Snapshot-Volume) zum Zwischenspeichern der alten Daten (siehe

http://tldp.org/HOWTO/LVM-HOWTO/snapshots_backup.html). Das Schreiben dieser Daten auf das Volume verursacht eine große Anzahl von I/O-Operationen auf dem entsprechenden Laufwerk. Aus diesem Grund ist das Backup üblicherweise langsamer, wenn ein Snapshot durch den LVM erfasst wird.

Falls Sie sich zur Verwendung des LVM entscheiden, erstellt Acronis Backup & Recovery 11.5 selbstständig ein logisches Snapshot-Volume. Die Software verfährt folgendermaßen:

1. Sie überprüft die gesicherte Volume-Größe (nicht die Datengröße, sondern die Volume-Größe).
2. Sie berechnet 10 Prozent dieser Größe – beispielsweise 10 GB.
3. Sie überprüft, ob mindestens 10 GB von 'nicht zugeordnetem' Speicherplatz auf der entsprechenden Volume-Gruppe vorhanden ist.
4. Falls dem so ist, erstellt Sie ein logisches Snapshot-Volume mit 10 GB (mit dem Befehl **`lvcreate -s`**) und startet das Backup. Anderenfalls führt die Software das Backup unter Verwendung eines Acronis-Snapshots durch.
5. Sie löscht das Snapshot-Volume wieder, sobald es nicht mehr benötigt wird.

Mehrere logische Volumes werden nacheinander gesichert. Die Software erstellt für jedes davon ein separates Snapshot-Volume mit der entsprechenden Größe. Es wird immer nur ein Snapshot-Volume zur gleichen Zeit gespeichert.

Sollten sich die Daten während der Snapshot-Erfassung extrem schnell ändern, dann geht dem logischen Snapshot-Volume der Speicher aus und wird das Backup fehlschlagen. Aus diesem Grund können Sie den Standardwert von 10 Prozent unter **/etc/Acronis/BackupAndRecovery.config** beliebig bis hinauf zu 100 Prozent ändern (was einen Erfolg dann garantiert).

So ändern Sie die Standardgröße eines logischen Snapshot-Volumes:

1. Entscheiden Sie, wie viel 'nicht zugeordneten' Speicherplatz Sie nutzen wollen. Falls Sie zwei oder mehr logische Volumes sichern wollen, sollte sich Ihre Wahl nach dem größten dieser Volumes richten.

   Tipp: *Um die Menge an 'nicht zugeordnetem' Speicherplatz auf einer Volume-Gruppe angezeigt zu bekommen, führen Sie den Befehl* ***`vgdisplay`*** *aus und betrachten Sie dann die Ausgabezeile* ***`Free PE / Size`****. Um die Größe von logischen Volumes angezeigt zu bekommen, führen Sie den Befehl* ***`lvdisplay`*** *aus und betrachten Sie die Ausgabezeilen* ***`LV Size`****.*

2. Öffnen Sie die Datei **/etc/Acronis/BackupAndRecovery.config** in einem Text-Editor.
3. Suchen Sie nach der Zeile **`<value name="MMSDirPath" type="TString">`**.
4. Geben Sie folgendes Fragment direkt vor dieser Zeile ein:

```
<key name="LVMSnapshots">
      <value name="MinimalVGFreeRelative" type="TString">
            20
      </value>
</key>
```

   In diesem Beispiel beträgt der neue Wert 20 Prozent. Es muss sich um eine ganze Zahl handeln.

5. Speichern Sie die Datei. Die neue Einstellung gelten ab dem nächsten Backup. Es muss kein Dienst neu gestartet werden.

4.7.14 Medienkomponenten

Diese Option ist für Windows- und Linux-Betriebssysteme wirksam, wenn das Ziel des Backups CDs, DVDs oder Blue-ray Discs (BD) sind.

Wenn Sie ein Backup auf ein solches Medium speichern, dann können Sie dieses Medium zu einem Linux-basierten bootfдhigen Medium (S. 487) machen, indem Sie zusätzliche Komponenten darauf speichern. Als Konsequenz benötigen Sie kein separates Notfallmedium.

Voreinstellung ist: **Keine bootfähigen Komponenten.**

Wählen Sie eine der folgenden Komponenten, die Sie auf das bootfähige Medium platzieren wollen:

- Der **Acronis Bootable Agent** ist ein bootfähiges, auf einem Linux-Kernel basierendes Notfallwerkzeug, das die meisten Funktionen des Acronis Backup & Recovery 11.5 Agenten enthält. Platzieren Sie diese Komponente auf dem Medium, wenn Sie größere Funktionalität während der Wiederherstellung wünschen. Sie können die Wiederherstellung auf die gleiche Weise wie von einem regulären Boot-Medium konfigurieren und Active Restore oder Universal Restore verwenden. Wenn das Medium in Windows erstellt wird, stehen auch die Funktionen zur Laufwerksverwaltung zur Verfügung.
- **Acronis Bootable Agent und One-Click Restore**. One-Click Restore ist eine kleine Ergänzung zu einem Laufwerk-Backup, das auf einem Wechselmedium gespeichert ist, welche auf einen einzelnen Klick hin eine Wiederherstellung dieses Backups ermöglicht. Wenn Sie eine Maschine von diesem Medium starten und auf **Acronis One-Click Restore ausführen** klicken, dann wird das Laufwerk unmittelbar aus dem Backup wiederhergestellt, das auf dem gleichen Medium enthalten ist.

  Achtung: *Weil diese Art der Wiederherstellung keine Interaktionaktionsmöglichkeit für den Benutzers bietet, wie z.B. die Auswahl der wiederherzustellenden Volumes, stellt Acronis One-Click Restore immer das komplette Laufwerk wieder her. Falls das Laufwerk also mehrere Volumes enthält und Sie den Einsatz von Acronis One-Click Restore planen, dann müssen Sie alle Volumes in das Backup aufnehmen. Ansonsten gehen beim Einsatz dieser Funktion die Volumes verloren, die nicht im Backup enthalten sind.*

4.7.15 Mount-Punkte

Diese Option ist nur unter Windows und für ein Datei-basiertes Backup wirksam, dessen Datenquelle gemountete Volumes oder freigegebene Cluster-Volumes enthält.

Diese Option ist nur wirksam, wenn Sie einen Ordner als Backup-Quelle auswählen, der in der Verzeichnishierarchie höher als der Mount-Punkt liegt. (Ein Mount-Punkt ist ein Ordner, an den ein zusätzliches Volume logisch angebunden ist).

- Wenn ein solcher Ordner (oder ein übergeordneter Ordner) als Backup-Quelle ausgewählt wird – und die Option **Mount-Punkte** aktiviert wurde – dann werden alle auf dem gemounteten Volume liegenden Dateien in das Backup aufgenommen. Wenn die Option **Mount-Punkte** deaktiviert wurde, bleibt der Mount-Punkt im Backup leer.

  Bei der Wiederherstellung eines übergeordneten Ordners hängt die Frage, ob auch der Inhalt des Mount-Punktes wiederhergestellt wird (oder nicht) davon ab, ob die Option **Mount-Punkte** fьr die Recovery-Aktion (S. 185) aktiviert oder deaktiviert wurde.
- Wenn Sie den Mount-Punkt direkt auswählen oder einen Ordner innerhalb des gemounteten Volumes, dann werden die gewählten Ordner wie herkömmliche Ordner betrachtet. Sie werden unabhängig vom Status der Backup-Option **Mount-Punkte** gesichert – genauso, wie sie unabhängig vom Status der entsprechenden Recovery-Option **Mount-Punkte**fьr die Recovery-Aktion (S. 185) wiederhergestellt werden.

Voreinstellung ist: **Deaktiviert**.

Tipp: *Sie können virtuelle Maschinen vom Typ Hyper-V sichern, die auf einem freigegebenen Cluster-Volume liegen, indem Sie die benötigten Dateien oder das komplette Volume per Datei-basiertem Backup sichern.*

Fahren Sie die virtuellen Maschinen herunter, um zu gewährleisten, dass sie in einem konsistenten Zustand gesichert werden.

Beispiel

Angenommen, der Ordner **C:\Daten1** ist der Mount-Punkt für ein gemountetes Volume. Das Volume enthält die Verzeichnisse **Ordner1** und **Ordner2**. Sie erstellen einen Backup-Plan zur Datei-basierten Sicherung Ihrer Daten.

Wenn Sie das Volume C per Kontrollkästchen auswählen und dafür die Option **Mount-Punkte** aktivieren, wird der Ordner **C:\Daten1** in Ihrem Backup auch die Verzeichnisse **Ordner1** und **Ordner2** enthalten. Wenn Sie die gesicherten Daten dann später wiederherstellen, sollten Sie an die entsprechende, gewünschte Einstellung der Option **Mount-Punkte** fьr die Recovery-Aktionen (S. 185) denken.

Wenn Sie das Volume C per Kontrollkästchen auswählen und die Option **Mount-Punkte** jedoch deaktivieren, wird der Ordner **C:\Daten1** in Ihrem Backup leer sein.

Wenn Sie die Verzeichnisse **Daten1**, **Ordner1** oder **Ordner2** direkt selbst per Kontrollkästchen zum Backup auswählen, werden diese markierten Ordner wie herkömmliche Ordners in Backup aufgenommen – unabhängig vom Status der Option **Mount-Punkte**.

4.7.16 Multi-Volume-Snapshot

Diese Option ist nur für Windows-Betriebssysteme wirksam.

Diese Option gilt für Backups auf Laufwerksebene. Diese Option gilt auch für Backups auf Dateiebene, wenn diese unter Verwendung eines Snapshots erstellt werden. (Die Option Snapshot fьr Backup auf Dateiebene (S. 127) bestimmt, ob bei einem solchen Backup ein Snapshot benutzt wird oder nicht.)

Die Option bestimmt, ob Snapshots mehrerer Volumes gleichzeitig oder einer nach dem anderen erfasst werden sollen.

Voreinstellung ist: **Aktivieren.**

Wenn diese Option auf **Aktivieren** gesetzt wird, werden die Snapshots aller zu sichernden Volumes zum gleichen Zeitpunkt erstellt. Benutzen Sie diese Option, um ein zeitkonsistentes Backup von Daten zu erstellen, die über mehrere Volumes verteilt sind, z.B. für eine Oracle-Datenbank.

Wenn diese Option auf **Deaktivieren** gesetzt wird, erfolgen die Snapshots der Volumes nacheinander. Falls sich also Daten über mehrere Volumes erstrecken, werden diese zu unterschiedlichen Zeiten gesichert und das resultierende Backup könnte nicht konsistent sein.

4.7.17 Benachrichtigungen

Acronis Backup & Recovery 11.5 kann Sie über den Abschluss eines Backups per E-Mail oder Windows Nachrichtendienst (WinPopup, nur bei Windows XP) benachrichtigen.

4.7.17.1 E-Mail

Diese Option ist für Windows- und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar, wenn Sie ein Boot-Medium gestartet haben und mit diesem arbeiten.

Die Option ermöglicht Ihnen den Erhalt von E-Mail-Benachrichtigungen über den erfolgreichen Abschluss von Backup-Tasks, über Fehler oder wenn ein Benutzereingriff erforderlich ist.

Voreinstellung ist: **Deaktiviert**.

So konfigurieren Sie eine E-Mail-Benachrichtigung

1. Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigung schicken**, um die entsprechende Funktion zu aktivieren.
2. Aktivieren Sie unter **E-Mail-Benachrichtigungen schicken** die entsprechenden Kontrollkästchen folgendermaßen:
   - **Wenn das Backup erfolgreich abgeschlossen wurde**.
   - **Wenn das Backup fehlschlägt**.
   - **Wenn Benutzereingriff erforderlich ist**.
3. Aktivieren Sie das Kontrollkästchen **Vollständiges Log zur Benachrichtigung hinzufügen**, falls Sie möchten, dass die E-Mail-Benachrichtigung Log-Einträge für die Aktion beinhalten soll.
4. Geben Sie die E-Mail-Adresse des Ziels im Feld **E-Mail-Adressen** ein. Sie können auch mehrere, per Semikolon getrennte Adressen eingeben.
5. Geben Sie im Feld **Betreff** eine Beschreibung für die Benachrichtigung ein.

   Die Betreffzeile kann gewöhnlichen Text und eine oder mehrere Variablen enthalten. In den empfangenen E-Mail-Nachrichten wird jede Variable dann durch den zum Zeitpunkt der Task-Ausführung vorliegenden Wert ersetzt. Folgende Variablen werden unterstützt:
   - **%description%**

     Bei einer unter Windows laufenden Maschine wird die Variable **%description%** durch einen Text ersetzt, der dem Feld **Computerbeschreibung** der jeweiligen Maschine entspricht. Um den Text spezifizieren zu können, können Sie entweder zu **Systemsteuerung –> System** gehen oder folgenden Befehl als Administrator ausführen:

     ```
     net config server /srvcomment:<text>
     ```

     Bei einer unter Linux laufenden Maschine wird die Variable **%description%** durch einen leeren String ("") ersetzt.
   - **%subject%**

     Die Variable **%subject%** wird in folgenden Ausdruck umgewandelt: *Task <Task-Name> <Task-Ergebnis> auf Maschine <Maschinenname>.*
6. Geben Sie im Feld **SMTP-Server** den Namen des ausgehenden Mail-Servers (SMTP) ein.
7. Legen Sie im Feld **Port** die Port-Nummer des ausgehenden Mail-Servers fest. Standardmäßig ist der Port auf **25** gesetzt.
8. Sollte der ausgehende Mail-Server eine Authentifizierung benötigen, dann geben Sie den **Benutzernamen** und das **Kennwort** vom E-Mail-Konto des Senders ein.

   Sollte der SMTP-Server keine Authentifizierung benötigen, dann lassen Sie die Felder **Benutzername** und **Kennwort** einfach leer. Falls Sie nicht sicher sind, ob Ihr SMTP-Server eine Authentifizierung erfordert, dann kontaktieren Sie Ihren Netzwerk-Administrator oder bitten Sie Ihren E-Mail-Dienstanbieter um Hilfe.
9. Klicken Sie auf **Erweiterte E-Mail-Parameter...**, um weitere E-Mail-Parameter folgendermaßen zu konfigurieren:
   a. **Von** – geben Sie den Namen des Absenders an. Falls Sie das Feld leer lassen, dann enthalten die Nachrichten im Feld **Von** das E-Mail-Konto des Senders.
   b. **Verschlüsselung verwenden** – Sie können sich für eine verschlüsselte Verbindung zum Mail-Server entscheiden. Zur Auswahl stehen die Verschlüsselungstypen SSL und TLS.

c. Einige Internetdienstanbieter verlangen eine Authentifizierung am Posteingangsserver, bevor das Verschicken von Nachrichten erlaubt wird. Wenn das bei Ihnen zutrifft, aktivieren Sie das Kontrollkästchen **Anmeldung beim Posteingangsserver**, um einen POP3-Server zu aktivieren und seine Einstellungen einzurichten:
   - **Posteingangsserver (POP3)** – geben Sie den Namen des POP3-Servers an.
   - **Port** – bestimmt den Port des POP3-Servers. Standardmäßig ist der Port auf **110** gesetzt.
   - **Benutzername** und **Kennwort** für den eingehenden Mail-Server.

d. Klicken Sie auf **OK**.

10. Klicken Sie auf **Test-Mail senden**, um zu überprüfen, ob die E-Mail-Benachrichtigungen mit den spezifizierten Einstellungen korrekt funktionieren.

4.7.17.2 Nachrichtendienst (WinPopup)

Diese Option ist wirksam für die Betriebssysteme Windows XP, Windows Server 2003 und Linux auf der sendenden Maschine – sowie für Windows XP oder Windows Server 2003 auf der empfangenden Maschine. Windows Vista und spätere Versionen von Windows unterstützen den Nachrichtendienst nicht mehr.

Diese Option ist nicht verfügbar, wenn Sie ein Boot-Medium gestartet haben und mit diesem arbeiten.

Die Option ermöglicht Ihnen den Erhalt von WinPopup-Benachrichtigungen über die erfolgreiche Vollendung von Backup-Tasks, über Fehler oder über erforderliche Handlungen.

Voreinstellung ist: **Deaktiviert.**
Vor Konfiguration der WinPopup-Benachrichtung sollten Sie sicherstellen, dass der Nachrichtendienst von Windows XP auf beiden Maschinen (die Task ausführende und die Nachrichten empfangende Maschine) gestartet ist.

Der Nachrichtendienst ist bei Windows XP SP2+ und Windows Server 2003/2003 R2 standardmäßig deaktiviert. Ändern Sie den **Starttyp** auf **Automatisch** und starten Sie den Dienst dann neu.

So konfigurieren Sie WinPopup-Benachrichtigungen:

1. Aktivieren Sie das Kontrollkästchen **WinPopup-Benachrichtigung schicken**.
2. Geben Sie in das Feld **Maschinenname** den Namen der Maschine ein, an die die Benachrichtigungen verschickt werden. Mehrere Namen werden nicht unterstützt.

Aktivieren Sie unter **Benachrichtigungen senden** die Kontrollkästchen folgendermaßen:

- **Wenn das Backup erfolgreich abgeschlossen wurde** – damit eine Benachrichtigung gesendet wird, wenn der Backup-Task erfolgreich abgeschlossen wurde
- **Wenn das Backup fehlschlägt** – zum Versenden einer Benachrichtigung, wenn die Backup-Aktion nicht erfolgreich abgeschlossen wird
- **Wenn Benutzereingriff erforderlich ist** – zum Versenden einer Benachrichtigung, wenn während der Aktion das Eingreifen des Benutzers erforderlich ist.

Klicken Sie auf **WinPopup-Testnachricht senden**, um die Richtigkeit der Einstellungen zu prüfen.

4.7.18 Vor-/Nach-Befehle

Diese Option ist für Windows-, Linux-Betriebssysteme und das PE-Boot-Medium wirksam.

Diese Option ermöglicht die Definition von Befehlen, die automatisch vor oder nach einem Backup durchgeführt werden.

Das folgende Schema zeigt, wann diese Befehle ausgeführt werden.

Befehl vor dem Backup	Backup	Befehl nach Backup

So benutzen Sie diese Vor- bzw. Nach-Befehle:

- Löschen Sie bestimmte temporäre Dateien von der Festplatte, bevor ein Backup gestartet wird.
- Konfiguration Sie das Antivirenprodukt eines Drittanbieters so, dass es vor jedem Start des Backups ausgeführt wird.
- Kopieren Sie Backups selektiv von einem Archiv zu einem anderen Speicherort. Diese Option kann nützlich sein, weil die in einem Backup-Plan konfigurierte Replikation *jedes* Backup eines Archivs zu den nachfolgenden Speicherorten kopiert.

Acronis Backup & Recovery 11.5 führt die Replikation *nach* Ausführung des Nach-Backup-Befehls aus. Weitere Informationen finden Sie unter 'Die Reihenfolge von Aktionen in einem Backup-Plan (S. 82)'.

Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern, wie z.B. „pause".

So spezifizieren Sie Vor-/Nach-Befehle

1. Sie aktivieren Vor-/Nach-Befehle mit Hilfe der folgenden Optionen:
   - **Vor Backup ausführen**
   - **Nach Backup ausführen**
2. Wählen Sie aus den nachfolgenden Varianten:
   - Klicken Sie auf **Bearbeiten**, um einen neuen Befehl oder eine Stapelverarbeitungsdatei zu spezifizieren.
   - Wählen Sie einen existierenden Befehl oder eine Stapelverarbeitungsdatei aus der Dropdown-Liste.
3. Klicken Sie auf **OK**.

4.7.18.1 Befehl vor Backup

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die vor dem Start des Backups ausgeführt wird

1. Tragen Sie im Eingabefeld **Befehl** einen Befehl ein oder suchen Sie eine vorbereitete Stapelverarbeitungsdatei. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. „pause").
2. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden.
3. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
4. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
5. Klicken Sie auf **Befehl testen**, um zu prüfen, ob der Befehl korrekt funktioniert.

Kontrollkästchen	**Auswahl**			
Task scheitern lassen, wenn die Befehlsausführung fehlschlägt*	Ausgewählt	Deaktiviert	Ausgewählt	Deaktiviert

Kein Backup, bis die Befehlsausführung abgeschlossen ist	Ausgewählt	Ausgewählt	Deaktiviert	Deaktiviert
		Ergebnis		
	Voreinstellung Backup nur ausführen, nachdem der Befehl erfolgreich durchgeführt wurde. Task scheitern lassen, wenn die Befehlsausführung fehlschlägt.	Backup nach Befehlsausführung fortsetzen, unabhängig vom Erfolg oder Misserfolg der Ausführung.	Nicht verfügbar	Backup gleichzeitig mit Befehlsausführung durchführen, unabhängig vom Ergebnis der Befehlssausführung.

* Ein Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist.

4.7.18.2 Befehl nach Backup

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die ausgeführt wird, wenn das Backup vollständig ist

1. Tragen Sie im Eingabefeld **Befehl** ein Kommando ein oder suchen Sie eine vorbereitete Stapelverarbeitungsdatei.
2. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden soll.
3. Tragen Sie, sofern erforderlich, in das Feld **Argumente** entsprechende Parameter für die Befehlsausführung ein.
4. Aktivieren Sie das Kontrollkästchen **Task scheitern lassen, wenn die Befehlsausführung fehlschlägt**, sofern eine erfolgreiche Ausführung des Befehls wichtig für Sie ist. Der Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist. Falls die Befehlsausführung versagt, wird das Programm die entstehende tib-Datei sowie temporäre Dateien sofern möglich entfernen – das Task-Ergebnis wird zudem auf 'Fehlgeschlagen' gesetzt.

   Wenn das Kontrollkästchen nicht ausgewählt ist, dann hat das Ergebnis der Befehlsausführung keinen Einfluss auf Erfolg oder Misserfolg des Tasks. Sie können das Ergebnis der Befehlsausführung durch Einsicht in das Log verfolgen – oder über die Fehler- bzw. Warnmeldungen, die in der Ansicht **Log** angezeigt werden.
5. Klicken Sie auf **Befehl testen**, um zu prüfen, ob der Befehl korrekt funktioniert.

4.7.19 Befehle vor/nach der Datenerfassung

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ermöglicht die Definition von Befehlen, die automatisch vor oder nach der Datenerfassung (also Erstellung des Daten-Snapshots) durchgeführt werden. Die Datenerfassung wird von Acronis Backup & Recovery 11.5 zu Beginn der Backup-Prozedur durchgeführt.

Das folgende Schema zeigt, wann diese Befehle ausgeführt werden.

	<--------------- **Backup** --------------->				
Befehl vor Backup	Befehl vor Datenerfassung	Datenerfassung	Befehl nach Datenerfassung		Befehl nach Backup

Wenn die Option Volume Shadow Copy Service (S. 142) aktiviert ist, werden die Ausführung der Befehle und die Aktionen von Microsofts VSS folgendermaßen eingeordnet:

Befehle „vor Datenerfassung“ -> VSS Suspend -> Datenerfassung -> VSS Resume -> Befehle „nach Datenerfassung“.

Mit Hilfe der Befehle vor bzw. nach der Datenerfassung können Sie Datenbanken, die nicht mit VSS kompatibel sind, vor der Datenerfassung suspendieren und nach der Datenerfassung wieder anlaufen lassen. Im Gegensatz zu den Vor-/Nach-Befehlen (S. 133) werden die Befehle vor/nach der Datenerfassung direkt vor bzw. nach dem Datenerfassungsprozess durchgeführt. Das benötigt einige Sekunden. Die komplette Backup-Prozedur kann in Abhängigkeit von der zu sichernden Datenmenge entsprechend deutlich länger dauern. Daher werden die Datenbanken oder die Anwendungen nur kurze Zeit pausieren.

So spezifizieren Sie Befehle vor/nach der Datenerfassung

1. Sie aktivieren Befehle vor/nach der Datenerfassung mit Hilfe der folgenden Optionen:
   - **Vor der Datenerfassung ausführen**
   - **Nach der Datenerfassung ausführen**
2. Wählen Sie aus den nachfolgenden Varianten:
   - Klicken Sie auf **Bearbeiten**, um einen neuen Befehl oder eine Stapelverarbeitungsdatei zu spezifizieren.
   - Wählen Sie einen existierenden Befehl oder eine Stapelverarbeitungsdatei aus der Dropdown-Liste.
3. Klicken Sie auf **OK**.

4.7.19.1 Befehl vor Datenerfassung

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die vor der Datenerfassung ausgeführt wird

1. Tragen Sie im Eingabefeld **Befehl** einen Befehl ein oder suchen Sie eine vorbereitete Stapelverarbeitungsdatei. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. „pause“).
2. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden.
3. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
4. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
5. Klicken Sie auf **Befehl testen**, um zu prüfen, ob der Befehl korrekt funktioniert.

Kontrollkästchen	**Auswahl**			
Backup-Task scheitern lassen, wenn die Befehlsausführung fehlschlägt*	Ausgewählt	Deaktiviert	Ausgewählt	Deaktiviert
Keine Datenerfassung, bis die Befehlsausführung abgeschlossen ist	Ausgewählt	Ausgewählt	Deaktiviert	Deaktiviert

Ergebnis				
	Voreinstellung Datenerfassung nur ausführen, nachdem der Befehl erfolgreich durchgeführt wurde. Task scheitern lassen, wenn die Befehlsausführung fehlschlägt.	Datenerfassung nach Befehlsausführung fortsetzen, unabhängig vom Erfolg oder Misserfolg der Ausführung.	Nicht verfügbar	Datenerfassung gleichzeitig mit Befehlsausführung durchführen, unabhängig vom Ergebnis der Befehlssausführung.

* Ein Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist.

4.7.19.2 Befehl nach Datenerfassung

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die nach der Datenerfassung ausgeführt wird

1. Tragen Sie im Eingabefeld **Befehl** einen Befehl ein oder suchen Sie eine vorbereitete Stapelverarbeitungsdatei. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. „pause“).
2. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden.
3. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
4. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
5. Klicken Sie auf **Befehl testen**, um zu prüfen, ob der Befehl korrekt funktioniert.

Kontrollkästchen	Auswahl			
Task scheitern lassen, wenn die Befehlsausführung fehlschlägt*	Ausgewählt	Deaktiviert	Ausgewählt	Deaktiviert
Kein Backup, bis die Befehlsausführung abgeschlossen ist	Ausgewählt	Ausgewählt	Deaktiviert	Deaktiviert
Ergebnis				
	Voreinstellung Backup nur fortsetzen, nachdem der Befehl erfolgreich durchgeführt wurde. Löschen der tib-Datei und temporären Dateien sowie Task fehlschlagen lassen, wenn die Befehlsausführung versagt.	Backup nach Befehlsausführung fortsetzen, unabhängig vom Erfolg oder Misserfolg der Ausführung.	Nicht verfügbar	Backup gleichzeitig mit Befehlsausführung fortsetzen, unabhängig vom Ergebnis der Befehlssausführung.

* Ein Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist.

4.7.20 Inaktivitätszeit für Replikation/Bereinigung

Diese Option ist nur wirksam, wenn Sie für Backups entweder Replikation oder Aufbewahrungsregeln (S. 104) einrichten.

Die Option definiert einen Zeitraum, in dem der Start einer Replikation oder die Anwendung von Aufbewahrungsregeln nicht erlaubt ist. Diese Aktionen werden daher dann ausgeführt, wenn die Inaktivitätszeit beendet ist und sofern die Maschine zu diesem Zeitpunkt eingeschaltet ist. Aktionen, die vor dem Inaktivitätszeitraum gestartet wurden, werden ohne Unterbrechung fortgesetzt.

Die Inaktivitätszeit betrifft alle Speicherorte, den primären eingeschlossen.

Voreinstellung ist: **Deaktiviert.**

Aktivieren Sie zur Spezifikation der Inaktivitätszeit das Kontrollkästchen **Replikation/Bereinigung in folgender Zeit nicht starten** und wählen Sie dann die Tage und den entsprechenden Zeitraum.

Anwendungsbeispiele

Sie können diese Option auf Wunsch verwenden, um den eigentlichen Backup-Prozess von der Replikation oder Bereinigung zu separieren. Nehmen Sie beispielsweise an, dass Sie Maschinen lokal sowie tagsüber sichern und die entsprechenden Backups dann zu einem Netzwerkordner replizieren. Stellen Sie die Inaktivitätszeit so ein, dass sie die reguläre Arbeitszeit enthält. Die Replikation wird daraufhin nach diesen Arbeitstunden gemacht, wenn auch die Netzwerklast geringer ist.

4.7.21 Sektor-für-Sektor-Backup

Die Option ist nur für Backups auf Laufwerksebene wirksam.

Aktivieren Sie das Kontrollkästchen **Sektor-für-Sektor sichern**, um von einem Laufwerk bzw. Volume auf physikalischer Ebene eine exakte Kopie zu erstellen. Das resultierende Backup wird die gleiche Größe wie das gesicherte Laufwerk haben (sofern die Option **Komprimierungsgrad** (S. 123) auf **Keine** eingestellt ist). Verwenden Sie das Sektor-für-Sektor-Backup, um Laufwerke mit nicht erkanntem oder nicht unterstütztem Dateisystem und anderen proprietären Datenformaten zu sichern.

4.7.22 Bandverwaltung

Diese Optionen sind wirksam, wenn es sich bei dem Backup-Ziel um ein Bandgerät handelt.

Einen separaten Bandsatz für jede Maschine verwenden

Voreinstellung ist: **Deaktiviert**.

Bänder innerhalb eines Pools können in so genannte **Bandsätze** gruppiert werden.

Falls Sie diese Option deaktiviert lassen, werden die Daten von verschiedenen Maschinen auf alle zu einem Pool gehörenden Bänder gesichert. Falls die Option aktiviert ist, werden die Bänder einer jeden Maschine auf einem separaten Bandsatz gespeichert.

Diese Option gilt für Backup zu einem Storage Node.

Datei-Recovery für auf Bändern gespeicherte Laufwerk-Backups aktivieren

Voreinstellung ist: **Deaktiviert**.

Falls dieses Kontrollkästchen aktiviert ist, erstellte die Software bei jedem Backup zusätzliche Dateien auf einem Festplattenlaufwerk der Maschine, an welche das Bandgerät angeschlossen ist.

Datei-Recovery von Laufwerk-Backups ist möglich, solange diese zusätzlichen Dateien intakt sind. Die Dateien werden automatisch gelöscht, wenn das Band, auf dem die entsprechenden Backups gespeichert sind, gelцscht (S. 237), entfernt (S. 241) oder überschrieben wird.

Die Speicherorte der zusätzlichen Dateien sind:

- In Windows XP und Server 2003: **%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation**.
- In Windows Vista und späteren Versionen von Windows: **%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation**.
- In Linux: **/var/lib/Acronis/BackupAndRecovery/TapeLocation**.

Der von diesen zusätzlichen Dateien belegte Speicherplatz hängt von der Anzahl der Dateien im entsprechenden Backup ab. Beim Voll-Backup eines Laufwerks mit ungefähr 20.000 Dateien (typisches Laufwerk-Backup einer Workstation) belegen die zusätzlichen Dateien ca. 150 MB. Das Voll-Backup eines Servers mit 250.000 Dateien kann etwa 700 MB an zusätzlichen Dateien erzeugen. Sollten Sie sicher sein, dass Sie die Wiederherstellung einzelner Dateien nicht benötigen, dann können Sie das Kontrollkästchen deaktiviert lassen, um Speicherplatz zu sparen.

Wenn Sie ein Single-Pass-Laufwerk- und Anwendungs-Backup (S. 350) konfigurieren, ist das Kontrollkästchen **Datei-Recovery für auf Bändern gespeicherte Laufwerk-Backups aktivieren** automatisch aktiviert. Sie können es nur deaktivieren, wenn Sie das Backup-Ziel ändern oder Single-Pass-Backups deaktivieren.

Falls die zusätzlichen Dateien während des Backups nicht erstellt wurden oder falls sie gelöscht wurden, dann können Sie sie immer noch durch erneutes scannen (S. 238) derjenigen Bänder erstellen, die das Backup enthalten. Das gilt nicht für Backups, die mit Acronis Backup & Recovery 11 Update 0 (Build 17318) oder früher erstellt wurden.

Bänder nach erfolgreichen Backups auswerfen

Voreinstellung ist: **Deaktiviert**.

Wird dieses Kontrollkästchen aktiviert, dann wirft die Software Bänder nach jedem erfolgreichen Backup aus. Falls, gemäß des Backup-Plans, dem Backup weitere Aktionen folgen (beispielsweise eine Backup-Validierung oder Replikation zu einem anderen Speicherplatz), dann wird das Band nach Abschluss dieser Aktionen ausgeworfen.

Ein Band nach Verwendung zurück in den Schacht verschieben

Voreinstellung ist: **Aktiviert**.

Falls Sie diese Option deaktivieren, verbleibt ein Band in dem Laufwerk, nachdem eine Aktion mit dem Band abgeschlossen wurde.

Werden diese Option und die Option **Bänder nach erfolgreichen Backups auswerfen** aktiviert, dann wird das Band ausgeworfen.

Immer ein freies Band verwenden

Die Software versucht standardmäßig ein Backup auf ein Band zu schreiben, das bereits Backups derselben Backup-Kette oder desselben Archivs enthält. Falls ein solches nicht auffindbar ist, sucht die Software nach einem Band aus demselben Bandsatz. (Bandsätze können durch Bandpools ermittelt werden, durch die Option **Einen separaten Bandsatz für jede Maschine verwenden** oder durch die Backup-Schemata GroЯvater-Vater-Sohn (S. 70) oder Тьrme von Hanoi (S. 76)). Wird kein Band desselben Bandsatzes gefunden, dann versucht die Software, ein freies Band zu verwenden.

Sie können durch Änderung folgender Einstellungen die Verwendung eines freien Bandes erzwingen.

- **Für jedes Voll-Backup**

Voreinstellung ist: **Deaktiviert**.

Wenn diese Option aktiviert ist, wird jedes Voll-Backup auf ein freies Band geschrieben.

- **Für jedes differentielle Backup** (nicht anwendbar bei Backups von Exchange-Daten)

Voreinstellung ist: **Deaktiviert**.

Wenn diese Option aktiviert ist, wird jedes differentielle Backup auf ein freies Band geschrieben. Zusätzlich wird jedes Voll-Backup auf ein freies Band geschrieben. Das Kontrollkästchen **Für jedes Voll-Backup** wird ausgewählt und deaktiviert.

- **Für jedes inkrementelle Backup** (oder Transaktionsprotokoll-Backup, bei Backups von Exchange-Daten)

Voreinstellung ist: **Deaktiviert**.

Wenn diese Option aktiviert ist, wird jedes inkrementelle Backup auf ein freies Band geschrieben. Zusätzlich wird jedes Voll-Backup und jedes differentielle Backup auf ein freies Band geschrieben. Die Kontrollkästchen **Für jedes Voll-Backup** und **Für jedes differentielle Backup** werden ausgewählt und deaktiviert.

Band im Laufwerk bei Erstellung eines Voll-Backups überschreiben

Voreinstellung ist: **Deaktiviert**.

Diese Option gilt nur für autonome Bandlaufwerke. Ist diese Option aktiviert, dann wird ein in das Laufwerk eingelegtes Band jedes Mal überschrieben, wenn ein Voll-Backup erstellt wird.

4.7.23 Task-Fehlerbehandlung

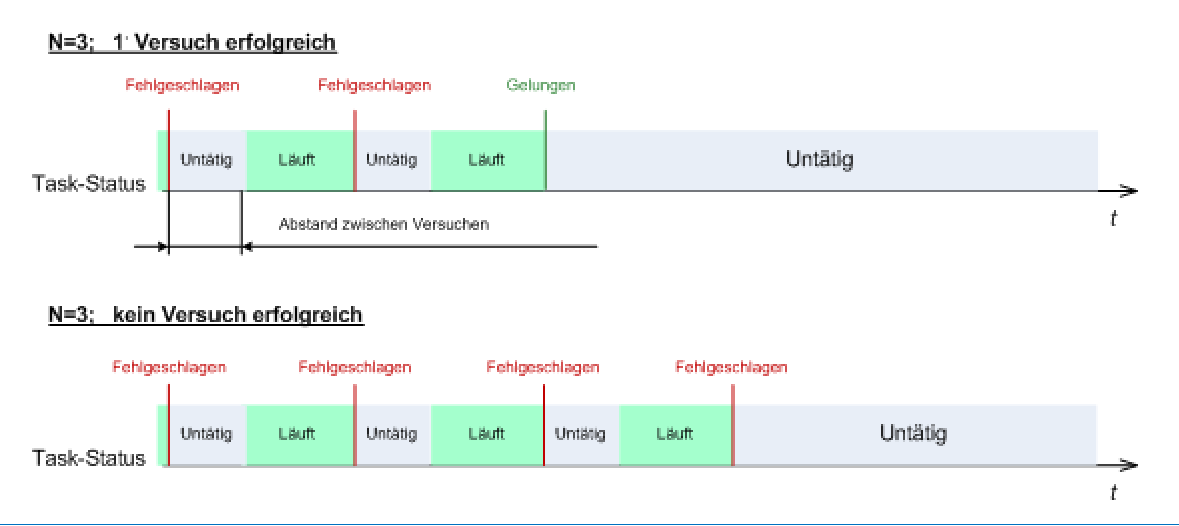
Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Diese Option bestimmt das Programmverhalten, wenn irgendein Task eines Backup-Plans versagt.

Die Voreinstellung ist **Fehlgeschlagenen Task nicht erneut starten.**

Wenn Sie das Kontrollkästchen **Fehlgeschlagenen Task erneut starten** aktivieren und die Anzahl der Versuche sowie den Zeitabstand zwischen den Versuchen angeben, versucht das Programm, den fehlgeschlagenen Task erneut zu starten. Die Versuche werden aufgegeben, wenn entweder die Aktion gelingt ODER die angegebene Zahl der Versuche erreicht ist, je nachdem, was zuerst eintritt.



Wenn ein Task aufgrund eines Fehlers im Backup-Plan fehlgeschlagen ist, können Sie den Plan bearbeiten, während der Task untätig ist. Während der Task dagegen läuft, müssen Sie ihn stoppen, bevor Sie den Backup-Plan bearbeiten können.

4.7.24 Task-Startbedingungen

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Diese Option bestimmt das Programmverhalten, falls ein Backup-Task starten will (die eingestellte Zeit ist gekommen oder das spezifizierte Ereignis ist eingetreten), aber die Bedingung (oder eine der Bedingungen) nicht erfüllt ist. Weitere Informationen über Bedingungen finden Sie unter Planen (S. 89) und Bedingungen (S. 100).

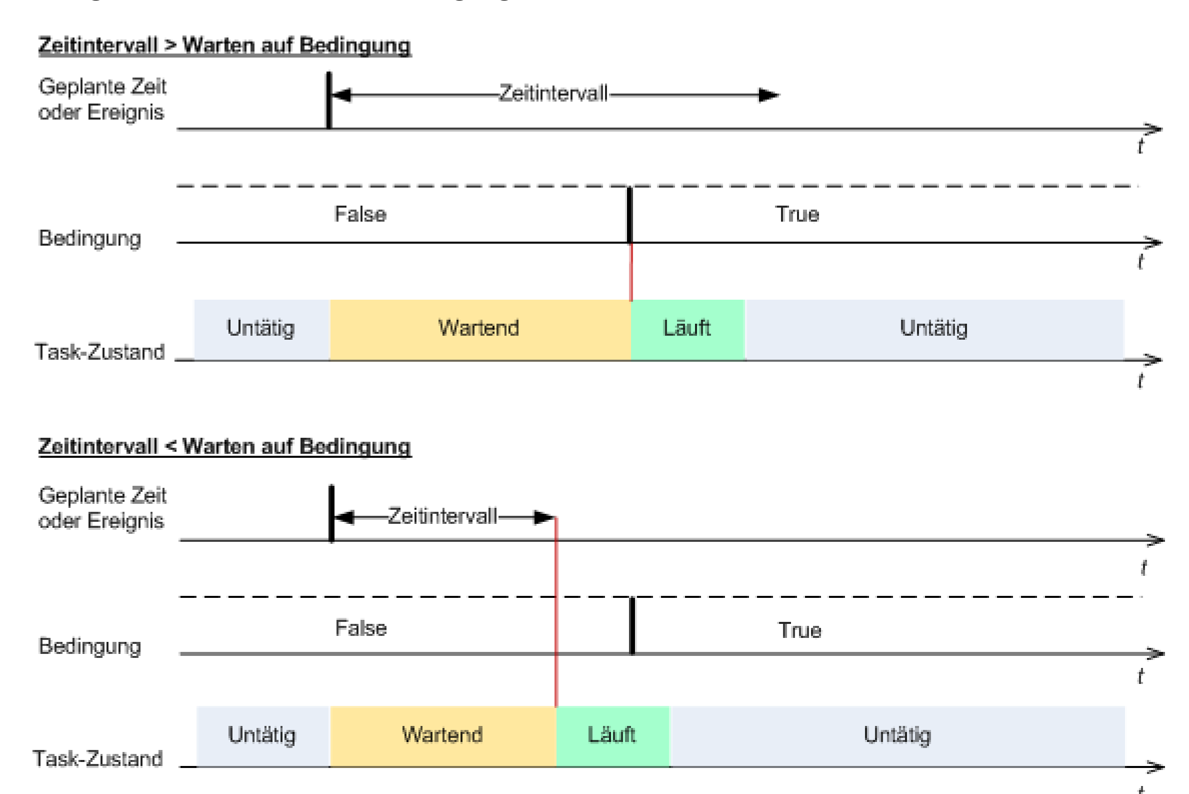
Voreinstellung ist: **Warten, bis die Bedingungen erfüllt sind.**

Warten, bis die Bedingungen erfüllt sind

Mit dieser Einstellung beginnt der Scheduler mit dem Überwachen der Bedingungen und schließt die Aufgabe ab, sobald die Bedingungen erfüllt sind. Wenn die Bedingungen nie erfüllt sind, wird der Task nie starten.

Um zu reagieren, wenn die Bedingungen für zu lange Zeit nicht erfüllt wurden und ein weiteres Verschieben des Backups zu riskant erscheint, können Sie einen Zeitabstand einstellen, nach dessen Ablauf der Task unabhängig von der Erfüllung der Bedingungen starten wird. Aktivieren Sie das Kontrollkästchen **Task trotzdem ausführen nach** und geben Sie dann den Zeitabstand an. Der Task wird starten, sobald die Bedingungen erfüllt sind ODER die Zeitspanne abgelaufen ist, je nachdem, was als Erstes eintritt.

Zeit-Diagramm: Warten, bis die Bedingungen erfüllt sind



Ausführung des Tasks übergehen

Das Verschieben eines Backups könnte nicht akzeptabel sein, wenn Sie z.B. ein Backup unbedingt zu einer angegebenen Zeit ausführen müssen. Dann macht es eher Sinn, das Backup zu übergehen, anstatt auf die Erfüllung der Bedingungen zu warten, besonders wenn die Ereignisse verhältnismäßig oft stattfinden.

4.7.25 Volume Shadow Copy Service

Diese Optionen sind nur für Windows-Betriebssysteme wirksam.

Den Volume Shadow Copy Service verwenden

Diese Option definiert, ob ein VSS-Provider (Volume Shadow Copy Service) VSS-kompatible Anwendungen benachrichtigen muss, dass ein Backup startet. Dies sichert einen konsistenten Zustand aller Daten, die von Anwendungen benutzt werden, vor allem aber die Vollendung aller Datenbanktransaktionen für den Moment, in dem Acronis Backup & Recovery 11.5 den Snapshot erstellt. Die Datenkonsistenz wiederum gewährleistet vor allem, dass Anwendungen in einem korrekten Zustand wiederhergestellt werden und unmittelbar nach der Wiederherstellung einsatzbereit sind.

Voreinstellung ist: **Volume Shadow Copy Service verwenden**.

VSS verwenden

Wenn die Option **Volume Shadow Copy Service verwenden** aktiviert ist, dann wählen Sie einen Snapshot-Provider aus folgender Liste:

- **Hardware/Software – Automatisch wählen**

VSS wird denjenigen Hardware-basierten Provider verwenden, der das Quell-Volume unterstützt. Wird keiner gefunden, dann verwendet der VSS den Acronis VSS Provider.

- **Software – Automatisch wählen**

  In den meisten Fällen wird der VSS den Acronis VSS Provider verwenden.

- **Software – Acronis VSS Provider**

  VSS wird den Acronis VSS Provider zum Erstellen von Snapshots verwenden.

- **Software – System-Provider** (standardmäßig voreingestellt)

  VSS wird den Provider des Systems (Microsoft Software Shadow Copy Provider) zum Erstellen von Snapshots verwenden. Wir empfehlen, beim Backup von Anwendungsservern (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint oder Active Directory) den System-Provider zu verwenden.

- **Software – Ein Software-Provider**

  In den meisten Fällen wird der VSS den Microsoft Software Shadow Copy Provider verwenden.

- **Hardware – Automatisch wählen**

  VSS wird denjenigen Hardware-basierten Provider verwenden, der das Quell-Volume unterstützt. Wird kein Hardware-basierter Provider gefunden, dann werden die Backups von Acronis Backup & Recovery 11.5 ohne die Erfassung von Snapshots erstellt.

***Hinweis:** Die Verwendung eines Hardware Snapshot Providers erfordert möglicherweise administrative Berechtigungen.*

VSS nicht verwenden

Wenn Sie die Option **VSS nicht verwenden** aktivieren, werden die Daten-Snapshots durch Acronis Backup & Recovery 11.5 erstellt.

Verwenden Sie die Option **VSS nicht verwenden**, wenn Ihre Datenbank mit VSS nicht kompatibel ist. Der Backup-Prozess ist am schnellsten, aber die Datenkonsistenz von Anwendungen, deren Transaktionen zum Zeitpunkt des Snapshots nicht vollendet sind, kann nicht garantiert werden. Sie können Befehle vor/nach der Datenerfassung (S. 135) verwenden, um festzulegen, welche Befehle vor und nach Erfassung des Snapshots ausgeführt werden sollen. Das gewährleistet, dass die Daten in einem konsistenten Zustand gesichert werden. Spezifizieren Sie z.B. einen Befehl vor der Datenerfassung, der diese Datenbank anhält und alle Cache-Speicher leert, um zu sichern, dass alle Transaktionen vollendet sind – und ergänzen Sie Befehle nach der Datenerfassung, damit die Datenbank nach der Snapshot-Erstellung den Betrieb wieder aufnimmt.

Über Volume Shadow Copy Writer

Bevor Sie die Daten einer VSS-kompatiblen Anwendung sichern, überprüfen Sie, dass die Volume Shadow Copy Writer für diese Anwendung eingeschaltet sind – und zwar, indem Sie die Liste der Writer untersuchen, die im Betriebssystem präsent sind. Verwenden Sie folgenden Befehl, um diese Liste einzusehen:

```
vssadmin list writers
```

***Hinweis:** In Microsoft Windows Small Business Server 2003 ist der Writer für Microsoft Exchange Server 2003 als Standardvorgabe ausgeschaltet. Informationen zum Anschalten des Schreibers finden Sie im Microsoft Knowledge Base-Artikel http://support.microsoft.com/kb/838183/.*

VSS-Voll-Backup aktivieren

Voreinstellung ist: **Deaktiviert**.

Diese Option kann nützlich sein, wenn Sie Microsoft Exchange-Server mit einem Laufwerk-Backup schьtzen (S. 318).

Sofern aktiviert, werden die Protokolle des Microsoft Exchange Servers und anderer VSS-kompatibler Anwendungen (mit Ausnahme des Microsoft SQL Servers) nach jedem erfolgreichen vollständigen, inkrementellen oder differentiellen Backup abgeschnitten.

Lassen Sie diese Option in folgenden Fällen deaktiviert:

- Falls Sie den Acronis Backup & Recovery 11.5 Agenten für Microsoft Exchange Server oder eine Dritthersteller-Software zum Backup von Exchange Server-Daten verwenden. Hintergrund ist, dass die Protokollabschneidung die aufeinanderfolgenden Transaktionsprotokoll-Backups beeinträchtigt.
- Falls Sie eine Dritthersteller-Software zum Backup der SQL Server-Daten verwenden. Hintergrund ist, dass die Dritthersteller-Software das resultierende Laufwerk-Backup als sein eigenes Voll-Backup ansehen wird. Als Folge wird das nächste differentielle Backup der SQL Server-Daten fehlschlagen. Die Backups werden solange fehlschlagen, bis die Dritthersteller-Software das nächste eigene Voll-Backup erstellt.
- Falls andere VSS-kompatible Anwendungen auf der Maschine laufen und es aus irgendwelchen Gründen notwendig ist, deren Protokolle zu behalten.

Eine Aktivierung dieser Option bewirkt kein Abschneiden von Microsoft SQL Server-Protokollen. Um das SQL Server-Protokoll nach einem Single-Pass-Backup (S. 345) (Einzeldurchlauf-Backup) abzuschneiden, müssen Sie die Einstellung **Protokollabschneidung** im Bereich **Single-Pass-Laufwerk- und Anwendungs-Backup** (S. 350) der Seite **Backup-Plan erstellen** oder **Backup jetzt** aktivieren.

Aktivieren Sie diese Option, wenn Sie VSS (virtueller Schattenkopie-Dienst) auf einer Maschine verwenden, die Windows XP verwendet und den Microsoft SQL Server ausführt. Falls Sie die Option deaktiviert lassen, kann das Backup fehlschlagen.

5 Recovery

Wenn eine Datenwiederherstellung ansteht, sollten Sie als Erstes erwägen, welches die funktionellste Methode ist: Verbinden Sie die Konsole mit der verwalteten, **das Betriebssystem ausführenden Maschine** und erstellen Sie den Recovery-Task.

Sollte auf der Maschine **das Betriebssystem nicht mehr starten** oder sollten Sie eine **Wiederherstellung auf fabrikneuer Hardware** durchführen müssen, dann booten Sie die Maschine mit einem bootfähigen Medium (S. 487) oder dem Acronis Startup Recovery Manager und konfigurieren Sie dann die Wiederherstellung.

Acronis Universal Restore ermöglicht Ihnen, Betriebssysteme **auf abweichender Hardware** oder einer virtuellen Maschine wiederherzustellen und von diesen zu booten.

Acronis Backup & Recovery 11.5 ermöglicht Ihnen, Windows-Betriebssystemen zwischen BIOS-basierter Hardware und UEFI-unterstütztender Hardware (Unified Extensible Firmware Interface) zu übertragen. Zu weiteren Details siehe den Abschnitt 'BIOS-basierte Systeme zu UEFI-basierten wiederherstellen und umgekehrt (S. 169)'.

Ein **Windows-System kann in Sekunden wieder online gebracht werden**, noch während die Wiederherstellung im Hintergrund abläuft. Dank der proprietären Technologie Acronis Active Restore (S. 173) kann Acronis Backup & Recovery 11.5 die Maschine in das im Backup vorliegende Betriebssystem 'hinein' booten – ganz so, als ob das System auf einer physikalischen Laufwerk vorliegen würde. Das System wird einsatzfähig und steht bereit, um notwendige Dienste anzubieten. Auf diese Weise bleibt die Ausfallszeit des Systems minimal.

Ein dynamisches Volume kann über ein bereits existierendes Volume, den 'nicht zugeordneten' Speicherplatz einer Laufwerksgruppe oder den 'nicht zugeordneten' Speicherplatz eines einzelnen Basis-Laufwerks wiederhergestellt werden. Um mehr über die Wiederherstellung dynamischer Volumes zu erfahren, wechseln Sie zum Abschnitt 'Backup und Recovery von dynamischen Volumes (Windows) (S. 43)'.

Zu detaillierten Informationen über die Wiederherstellung von Linux Software-RAID-Geräten und Volumes, die durch den LVM (Logical Volume Manager) erstellt wurden, siehe den Abschnitt 'MD-Geräte und logische Volumes wiederherstellen (S. 48)'.

Der Acronis Backup & Recovery 11.5 Agent für Windows und der Agent für Linux haben die Fähigkeit, ein Laufwerk- bzw. Volume-Backup zu einer neuen virtuellen Maschine wiederherzustellen. Mit dem Acronis Backup & Recovery 11.5 Agenten für Hyper-V oder dem Agenten für ESX(i) können Sie die neue virtuelle Maschine auf dem entsprechenden Virtualisierungsserver erstellen lassen. Weitere Informationen finden Sie im Abschnitt 'Wiederherstellung mit dem Ziel 'Neue virtuelle Maschine' (S. 196).

Sie müssen möglicherweise vor einer Wiederherstellung die Ziellaufwerke vorbereiten. Acronis Backup & Recovery 11.5 enthält ein nützliches Werkzeug zur Laufwerksverwaltung, welches Ihnen erlaubt, Volumes zu erstellen oder zu löschen, das Partitionsschema eines Laufwerks zu ändern, eine Laufwerksgruppe zu erstellen und andere Laufwerksverwaltungsaktionen auf der Ziel-Hardware durchzuführen (unter einem Betriebssystem oder direkt auf einem fabrikneuen System). Zu weiteren Informationen über Acronis Disk Director LV siehe den Abschnitt 'Laufwerksverwaltung (S. 300)'.

5.1 Einen Recovery-Task erstellen

Zur Erstellung eines Recovery-Tasks führen Sie folgende Schritte aus

Recovery-Quelle

Daten wählen (S. 147)

Wählen Sie die wiederherzustellenden Daten.

Anmeldedaten (S. 153)

[Optional] Stellen Sie Anmeldedaten für den Speicherort des Archivs zur Verfügung, falls das Benutzerkonto des Tasks für diesen keine Zugriffserlaubnis hat. Klicken Sie auf **Anmeldedaten anzeigen**, um auf diese Option zugreifen zu können.

Recovery-Ziel

Dieser Abschnitt erscheint, nachdem das benötigte Backup gewählt und der wiederherzustellende Datentyp definiert wurde. Die von Ihnen hier anzugebenden Parameter hängen vom wiederherzustellenden Datentyp ab.

Laufwerke (S. 154)

Volumes (S. 158)

Dateien (S. 162)

Microsoft Exchange-Datenbanken oder Speichergruppen

Microsoft Exchange-Postfächer oder Öffentliche Ordner

Microsoft SQL-Datenbanken (S. 350)

Microsoft Active Directory (S. 359)

[Nur auf dem Management Server] Wählen Sie die registrierte Maschine, die als Ziel für die wiederherzustellenden Daten dienen soll. In den meisten Fällen wird die Maschine automatisch ausgewählt, von der die Daten kommen. Falls Sie als Ziel für die Datenwiederherstellung eine Netzwerkfreigabe oder virtuelle Maschine verwenden müssen, dann wählen Sie die registrierte Maschine mit demjenigen Agenten, der die Recovery-Aktion durchführen soll.

Acronis Active Restore

[Optional] Aktivieren Sie Acronis Active Restore, falls es für Sie notwendig ist, ein System oder eine Datenbank bereits direkt nach dem Start der Wiederherstellung online zu bringen. Verfügbar für die Wiederherstellung von Windows (S. 173), Microsoft Exchange-Datenbanken oder Microsoft SQL-Datenbanken (S. 352).

Anmeldedaten (S. 153)

[Optional] Stellen Sie die Anmeldedaten für den Zielort zur Verfügung, falls mit den Anmeldedaten des Tasks keine Wiederherstellung der Daten möglich ist. Klicken Sie auf **Anmeldedaten anzeigen**, um auf diese Einstellung zugreifen zu können.

Recovery-Zeitpunkt

Recovery (S. 163)

Bestimmen Sie, wann die Wiederherstellung beginnen soll. Der Task kann unmittelbar nach Erstellung starten, für einen bestimmten Tag bzw. Zeitpunkt geplant werden oder auch einfach nur zur manuellen Ausführung gespeichert werden.

Task-Parameter

Task-Name

[Optional] Geben Sie einen eindeutigen Namen für den Recovery-Task ein. Ein bewusst gewählter Name macht es leichter, diesen Task zu identifizieren.

Recovery-Optionen

[Optional] Passen Sie die Aktion durch Konfiguration der Recovery-Optionen an, z.B. Vor-/Nach-Befehle, Recovery-Priorität, Fehlerhandhabung oder Benachrichtigungsoptionen. Sofern Sie in diesem Abschnitt nichts tun, werden die Standardwerte (S. 179) verwendet.

Wird irgendeine Einstellung gegenüber dem Standardwert geändert, so wird der neue Wert in einer neuen Zeile angezeigt. Die Statusanzeige über die Einstellungen ändert sich von **Standard** zu **Benutzerdefiniert**. Sollten Sie die Einstellung erneut ändern, so wird die Zeile ebenfalls den neuen Wert anzeigen, sofern er nicht dem Standardwert entspricht. Wenn der Standardwert eingestellt wird, verschwindet die Zeile. Sie sehen daher in diesem Abschnitt immer nur die Einstellungen, die von den Standardwerten abweichen.

Ein Klick auf **Auf Standard zurücksetzen** setzt alle Einstellungen auf die Standardwerte zurück.

Anmeldedaten für den Task

[Optional] Der Task wird im Namen des Benutzers laufen, der den Task erstellt. Sie können, sofern notwendig, die Konto-Anmeldedaten für den Task ändern. Klicken Sie auf **Anmeldedaten des Tasks anzeigen**, um auf diese Einstellung zugreifen zu können.

[Optional] Universal Restore für Windows/Linux

Angewendet auf: Recovery von Systemlaufwerken oder Volumes. Die Nutzung von Acronis Universal Restore erfordert eine separate Lizenz.

Universal Restore für Windows/Linux (S. 165)

Verwenden Sie Acronis Universal Restore, wenn Sie ein Betriebssystem auf abweichender Hardware wiederherstellen und booten müssen.

Klicken Sie nach Abschluss aller notwendiger Schritte auf **OK**, um den Recovery-Task zu erstellen.

5.1.1 Recovery-Quelle

1. Spezifizieren Sie den Archiv-Speicherort

Spezifizieren Sie im Feld **Datenpfad** den Pfad zum Archiv-Speicherort oder klicken Sie auf **Durchsuchen** und wählen Sie den gewünschten Speicherort (wie im Abschnitt 'Speicherort fьr Archive wдhlen (S. 149)' beschrieben) aus.

In den Advanced-Editionen von Acronis Backup & Recovery 11.5 können Sie den Archiv-Speicherort entweder wie gerade beschrieben spezifizieren oder den zentralen Datenkatalog verwenden.

2. Daten wählen

Sie können die gesicherten Daten entweder über die Registerlasche **Datenanzeige** oder **Archiv-Anzeige** auswählen. In der Registerlasche **Datenanzeige** werden alle gesicherten Daten innerhalb des gewählten Archiv-Speicherortes nach Versionen angezeigt (also dem Zeitpunkt der Backup-Erstellung). In der Registerlasche **Archiv-Anzeige** werden die gesicherten Daten nach Archiven angezeigt.

Daten in der Datenanzeige auswählen

Da die Registerlasche **Datenanzeige** seine Funktionalität mit dem Datenkatalog teilt, erfolgt die Datenauswahl in der Registerlasche **Datenanzeige** genauso wie im Datenkatalog. Zu weiteren Informationen über die Datenauswahl siehe daher 'Datenkatalog (S. 150)'.

Daten in der Archiv-Anzeige auswählen

1. Erweitern Sie das gewünschte Archiv und wählen Sie dann eines der aufeinander folgenden Backups anhand seines Zeitstempels. Auf diese Weise können Sie die Daten der Festplatte auf einen bestimmten Zeitpunkt zurücksetzen.

   Sollte die Liste der Archive nicht angezeigt werden (weil beispielsweise die Archiv-Metadaten verloren gingen), dann klicken Sie auf **Aktualisieren**.

   Falls die Liste der Archive zu lang ist, können Sie diese filtern, indem Sie festlegen, dass nur ein gewünschter Typ von Archiven angezeigt werden soll. Wählen Sie dazu den gewünschten Archivtyp in der Liste **Anzeigen**.

   Hinweis für Microsoft Exchange-Benutzer: *Informationen über die Auswahl von Microsoft Exchange-Daten finden Sie im Abschnitt 'Wahl der Exchange-Daten durch Verwendung der Archiv-Anzeige' der Dokumentation 'Backups von Microsoft Exchange-Server-Daten'.*

2. Nur für Laufwerk- oder Volume-Backups: Bestimmen Sie unter **Backup-Inhalt** den darzustellenden Datentyp aus dem Listenfeld:
   - **Laufwerke** – zur Wiederherstellung kompletter Laufwerke (mit all ihren Volumes).
   - **Volumes** – zur Wiederherstellung einzelner Volumes vom Typ 'Basis' oder 'Dynamisch'.
   - **Dateien** – zur Wiederherstellung einzelner Dateien und Ordner.
   - **Microsoft SQL-Datenbanken** – zur Wiederherstellung von Microsoft SQL-Datenbanken von Single-Pass-Laufwerk- und Anwendungs-Backups.
   - **Microsoft Active Directory** – zum Extrahieren von Microsoft Active Directory-Daten aus Single-Pass-Laufwerk- und Anwendungs-Backups.
3. Aktivieren Sie bei **Backup-Inhalt** die Kontrollkästchen der Elemente, die Sie wiederherstellen müssen.
4. Klicken Sie auf **OK**.

MBR wählen

Sie wählen bei Wiederherstellung eines System-Volumes den MBR des Laufwerks üblicherweise dann, wenn:

- Das Betriebssystem nicht booten kann.
- Das Laufwerk neu ist und keinen MBR hat.
- Sie benutzerdefinierte oder Nicht-Windows-Boot-Loader (wie LILO und GRUB) wiederherstellen.
- Die Laufwerksgeometrie von der im Backup gespeicherten abweicht.

Es gibt vermutlich noch andere Situationen, bei denen Sie den MBR wiederherstellen müssen, aber die oberen sind die häufigsten.

Bei Wiederherstellung eines MBR von einem auf ein anderes Laufwerk stellt Acronis Backup & Recovery 11.5 auch Track 0 (Spur Null) wieder her, was keinen Einfluss auf die Partitionstabelle und das Partitionslayout des Ziellaufwerks hat. Acronis Backup & Recovery 11.5 aktualisiert nach einer Wiederherstellung automatisch die Windows Boot-Loader, daher ist es bei Windows-Systemen nicht notwendig, den MBR und Track 0 wiederherzustellen, außer der MBR ist beschädigt.

5.1.1.1 Speicherort für Archive wählen

Speicherort	Details
Online Backup Storage	Falls das Archiv auf dem Acronis Online Backup Storage gespeichert wurde, klicken Sie auf **Anmelden** und geben Sie anschließend die Anmeldedaten zum Zugriff auf den Online Storage ein. Erweitern Sie dann die Gruppe **Online Backup Storage** und wählen Sie das Konto. *Auf dem Acronis Online Backup Storage gespeicherte Backups können nicht exportiert oder gemountet werden.*
Persönlich	Falls das Archiv in einem persönlichen Depot gespeichert ist, dann erweitern Sie die Gruppe **Persönlich** und klicken Sie auf das entsprechende Depot.
Zentral	Falls das Archiv in einem zentralen Depot gespeichert ist, dann erweitern Sie die Gruppe **Zentral** und klicken Sie auf das entsprechende Depot.
Maschinenname	Lokale Maschine
Lokale Ordner	Sollte das Archiv in einem lokalen Ordner auf der Maschine gespeichert sein, dann erweitern Sie die Gruppe **<Maschinenname>** und wählen Sie das gewünschte Verzeichnis.
CD, DVD, BD	Falls das Archiv auf optischen Medien wie CDs, DVDs oder Blu-ray-Medien (BD) gespeichert ist, dann erweitern Sie die Gruppe **<Maschinenname>** und wählen Sie das gewünschte Laufwerk aus. Legen Sie zuerst den letzten Datenträger ein. Legen Sie die Medien dann nach Anforderung des Programms nacheinander ein, beginnend mit dem ersten Medium.
RDX, USB	Falls das Archiv auf einem RDX- oder USB-Flash-Laufwerk gesichert ist, dann erweitern Sie die Gruppe **<Maschinenname>** und wählen Sie das gewünschte Laufwerk aus. Weitere Informationen über die Verwendung dieser Laufwerke finden Sie im Abschnitt 'Wechsellaufwerke (S. 221)'.
Bandgerät	Falls die Daten auf einem lokal angeschlossenen Bandgerät gespeichert sind, dann erweitern Sie die Gruppe **Bandgeräte** und klicken Sie dann auf das benötigte Gerät. In den Standalone-Editionen von Acronis Backup & Recovery 11.5 stehen Bandgeräte nur zur Verfügung, wenn Sie ein Upgrade von Acronis Backup & Recovery 10 durchgeführt haben. Zu weiteren Informationen über die Verwendung von Bändern siehe den Abschnitt 'Bandgerдte (S. 223).
Netzwerkordner	Wenn das Archiv auf einer Netzwerkfreigabe gespeichert ist, erweitern Sie die Gruppe **Netzwerk-Ordner**, wählen dann die benötigte Netzwerk-Maschine und klicken dann auf den freigegebenen Ordner. Werden Anmeldedaten zum Zugriff auf die Netzwerkfreigabe benötigt, so wird das Programm diese erfragen. ***Hinweis für Linux-Benutzer:*** *Um eine CIFS-Netzwerkfreigabe (Common Internet File System) anzugeben, die an einen Mount-Punkt (etwa /mnt/share) angeschlossen ist, wählen Sie diesen Mount-Punkt statt der Netzwerkfreigabe aus.*

Speicherort	Details
FTP, SFTP	Sollte das Archiv auf einem FTP- oder SFTP-Server gespeichert sein, dann geben Sie den Namen oder die Adresse des Servers folgendermaßen in das Feld **Pfad** ein: **ftp://ftp-server:port-nummer oder sftp://sftp-server:port-nummer** Verwenden Sie folgende Schreibweise, um eine FTP-Verbindung im aktiven Modus aufzubauen: **aftp://ftp-server:port-nummer** Wenn Sie die Port-Nummer nicht angeben, wird Port 21 für FTP benutzt und Port 22 für SFTP. Nach Eingabe der Anmeldedaten sind die Ordner auf dem Server verfügbar. Klicken Sie auf den passenden Ordner auf dem Server. Sie können auf den Server auch als anonymer Benutzer zugreifen, wenn der Server einen solchen Zugang ermöglicht. Dafür klicken Sie auf **Anonymen Zugang benutzen** anstelle der Eingabe von Anmeldedaten. *Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Klartext über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Packet-Sniffer abgefangen werden.*
Storage Nodes	Beim Arbeiten im Betriebssystem erfolgt der Zugriff auf einen Storage Node durch Wahl des entsprechenden zentralen Depots. Bei Ausführung auf einer Maschine, die mit einem bootfähigen Medium gestartet wurde: ▪ Um auf ein verwaltetes Depot zuzugreifen, geben Sie im Feld **Pfad** ein: **bsp://knoten_adresse/depot_name/** ▪ Um auf ein zentrales, nicht verwaltetes Depot zuzugreifen, tragen Sie den vollen Pfad zum Ordner des Depots ein.
NFS-Laufwerke	Falls das Archiv in einer NFS-Freigabe gespeichert ist, dann erweitern Sie die Gruppe **NFS-Laufwerke** und klicken Sie auf den entsprechenden Ordner. Nur unter Linux und unter Linux-basierten bootfähigen Medien verfügbar.

5.1.1.2 Datenkatalog

Der Datenkatalog ermöglicht Ihnen, die benötigten Versionen bestimmter Daten leicht zu finden und diese für eine Recovery-Aktion auszuwählen. Auf einer verwalteten Maschine ist die Datenkatalogfunktionalität für jedes Depot, auf das von dieser Maschine zugegriffen werden kann, über die Registerlasche **Datenanzeige** verfügbar. Auf dem Management Server ist die Katalogfunktionalität sowohl über die **Datenanzeige** wie auch den zentralen **Datenkatalog** verfügbar. Der zentrale Datenkatalog zeigt in einer Ansicht alle Daten an, die in den zentral verwalteten Depots gespeichert sind.

Acronis Backup & Recovery 11.5 lädt unter Umständen Datenkatalogdateien von einem Depot in einen lokalen Cache-Ordner. Dieser Ordner befindet sich standardmäßig auf dem Laufwerk, auf dem auch das Betriebssystem installiert ist. Informationen zur Änderung des vorgegebenen Cache-Ordners finden Sie im Abschnitt 'Den Standard-Cache-Ordner fьr Katalogdateien дndern (S. 216)'.

Gespeicherte Daten für eine Recovery-Aktion auswählen

1. Wählen Sie aus den nachfolgenden Varianten:

- Verbinden Sie zum Zugriff auf die Registerlasche **Datenanzeige** die Konsole mit einer Maschine oder dem Management Server, wechseln Sie zur Ansicht **Depots** und klicken Sie auf das benötigte Depot.
- Verbinden Sie zum Zugriff auf den **Datenkatalog** die Konsole mit dem Management Server und wählen Sie dann den **Datenkatalog** aus dem Verzeichnisbaum **Navigation** aus.

2. Bestimmen Sie im Feld **Anzeigen** den darzustellenden Datentyp:
   - Wählen Sie **Maschinen/Laufwerke/Volumes**, um vorliegende laufwerkbasierte Backups nach kompletten Laufwerken und Volumes durchsuchen zu können.
   - Wählen Sie **Dateien/Ordner**, um vorliegende Datei- und Laufwerk-Backups nach Dateien und Ordnern durchsuchen zu können.
   - Wählen Sie den **Microsoft Exchange-Informationsspeicher**, um nach Informationsspeichern, einzelnen Speichergruppen oder Datenbanken in Backups auf Datenbankebene suchen zu können.

     Wählen Sie **Microsoft Exchange-Postfächer**, um nach kompletten Postfächern, Öffentlichen Ordnern, einzelnen Ordnern, E-Mails, Kalenderereignissen, Aufgaben, Kontakten, Notizen in Backups auf Datenbank- und Postfachebene suchen zu können.

     Informationen über die Auswahl von Microsoft Exchange-Daten finden Sie im Abschnitt 'Wahl der Exchange-Daten durch Verwendung der Datenanzeige oder des Datenkatalogs' der Dokumentation 'Backups von Microsoft Exchange-Server-Daten'.
   - Wählen Sie **Microsoft SQL-Datenbanken**, um Microsoft SQL-Datenbanken in Single-Pass-Laufwerk- und Anwendungs-Backups durchsuchen zu können.
   - Wählen Sie **Microsoft Active Directory**, um Microsoft Active Directory-Daten in Single-Pass-Laufwerk- und Anwendungs-Backups zu suchen.
3. Spezifizieren Sie im Feld **Backups anzeigen für** den gewünschten Zeitraum, für den die gespeicherten Daten angezeigt werden sollen.
4. Wählen Sie aus den nachfolgenden Varianten:
   - Wählen Sie die wiederherzustellenden Daten aus dem Katalogverzeichnis oder in der rechts neben diesem liegenden Tabelle.
   - Binden Sie diejenigen Informationen in den Suchstring mit ein, die Ihnen helfen, die benötigten Datenelemente (das kann ein Maschinenname, ein Ordnername oder eine Laufwerksbezeichnung sein) zu identifizieren – und klicken Sie dann auf den Befehl **Suchen**. Sie können die Wildcards Sternchen (*) und Fragezeichen (?) verwenden.

     Als Ergebnis sehen Sie im Fenster **Suchen** eine Liste mit all den gespeicherten Datenelementen, deren Namen vollständig oder teilweise mit dem eingegebenen Wert übereinstimmt. Sollte die Liste der Suchtreffer zu lang sein, dann können Sie die Suchkriterien verfeinern, beispielsweise indem Sie Datum bzw. Zeit der Backup-Erstellung und/oder einen Größenbereich für die gespeicherten Elemente angeben. Wenn die benötigten Daten gefunden sind, wählen Sie diese aus und klicken Sie dann auf **OK**, um zurück zum/zur **Datenkatalog/Datenanzeige** zu gelangen.
5. Verwenden Sie die Liste der **Versionen**, um den Zeitpunkt zu bestimmen, zu dem hin die Daten wiederhergestellt werden sollen. Standardmäßig werden die Daten auf den jüngsten Zeitpunkt zurückgesetzt, der für den im Schritt 3 gewählten Zeitraum verfügbar ist.

   [Optional, nur für den **Datenkatalog** anwendbar] Falls es zu den Backup-Daten mehrere, an mehr als einem Ort gespeicherte Replikate gibt, dann können Sie auch den Ort auswählen, von dem aus (als Quelle) die Daten wiederhergestellt werden sollen. Wenn Sie Informationen über die Speicherorte der gewählten Daten haben wollen, dann klicken Sie mit der rechten Maustaste auf die gewünschte Version und wählen Sie **Das Depot ändern, von dem aus wiederhergestellt wird**.

Standardmäßig wird der Speicherort ausgewählt, der den schnellsten Zugriff auf die Daten bietet. Lokale Festplattenlaufwerke sind die schnellsten, Bänder die langsamsten.

6. Klicken Sie nach Auswahl der benötigten Daten auf **Recovery** und konfigurieren Sie dann die Parameter für die Wiederherstellungsaktion.

Was, wenn die Daten nicht im Katalog oder der Datenanzeige erscheinen?

Die wahrscheinlichen Gründe für dieses Problem sind:

Es wurde ein falscher Zeitraum eingestellt

Die benötigten Daten wurden während des Zeitraums, der über den Befehl **Backups anzeigen für** eingestellt wurde, nicht als Backup gesichert.

Lösung: Versuchen Sie, den Zeitraum zu vergrößern.

Katalogisierung ist deaktiviert oder die schnelle Katalogisierung ist angeschaltet

Falls die Daten nur teilweise oder überhaupt nicht angezeigt werden, war vermutlich die Katalogisierung deaktiviert oder während des Backups die schnelle Katalogisierung (S. 119) eingeschaltet.

Lösungen:

- Falls die Katalogisierung deaktiviert ist
    - Auf einer verwalteten Maschine: Aktivieren Sie die Katalogisierung mit der Option **Backup-Katalogisierung** (**Optionen** –> **Maschinen-Optionen**).
    - Auf dem Management Server: Aktivieren Sie die Katalogisierung durch Дnderung der Windows-Registry.
    - Auf dem/den Storage Node(s): Aktivieren Sie die Katalogisierung durch Дnderung der Windows-Registry.
- Führen Sie die vollständige Katalogisierung manuell aus, indem Sie auf **Jetzt katalogisieren** klicken. Für den **Datenkatalog** werden alle in den verwalteten Depots gespeicherten Backups katalogisiert. Für die Registerkarte **Datenanzeige** werden nur die auf dem gewählten Depot gespeicherten Backups katalogisiert. Zuvor bereits katalogisierte Backups werden nicht erneut katalogisiert.
- Da die Katalogisierung einer großen Anzahl an gespeicherten Daten längere Zeit benötigen kann, können Sie auf Wunsch auch die **Archiv-Anzeige** des entsprechenden Depots verwenden. Zu weiteren Informationen über die Verwendung der **Archiv-Anzeige** siehe den Punkt 'Depot-Inhalte durchsuchen und Datenauswahl' im Abschnitt 'Mit Depots arbeiten (S. 202)'.

Nicht vom Katalog unterstützte Daten

Folgende Daten können nicht im Katalog oder der Datenanzeige dargestellt werden:

- Daten aus verschlüsselten und kennwortgeschützten Archiven.
- Daten von verschlüsselten, verwalteten Depots.
- Daten, die als Backup auf Wechselmedien wie CDs, DVDs, BDs, Iomega REV, RDX oder USB-Geräten gespeichert wurden.
- Daten, die zum Acronis Online Backup Storage gesichert wurden.
- Daten, die mit Acronis True Image Echo oder früheren Versionen gesichert wurden.
- Daten, die mit vereinfachter Dateibenennung gesichert wurden.

Lösung: Verwenden Sie die Registerlasche **Archiv-Anzeige** des entsprechenden Depots, um solche Daten durchsuchen zu können.

Daten, die nicht im zentralen Katalog enthalten sind

Der zentrale Katalog zeigt keine Daten aus zentralen, nicht verwalteten Depots oder aus persцnlichen Depots (S. 213) an.

Lösung für zentrale, nicht verwaltete Depots: Wählen Sie das Depot im Verzeichnisbaum **Navigation** und wählen Sie dann die **Datenanzeige**.

Lösung für persönliche Depots: Verbinden Sie sich direkt mit der Maschine, wählen Sie das Depot und wählen Sie dann die **Datenanzeige**.

5.1.2 Anmeldedaten für den Speicherort

Spezifizieren Sie die Anmeldedaten, die notwendig sind, um auf den Ort zuzugreifen, wo die Backups gespeichert sind.

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Anmeldedaten des Tasks benutzen**

     Die Software greift auf den Speicherort mit den Anmeldedaten des Task-Kontos zu, wie sie im Abschnitt **Task-Parameter** spezifiziert wurden.
   - **Folgende Anmeldedaten verwenden**

     Die Software greift auf den Speicherort unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu. Verwenden Sie diese Option, wenn das Konto des Tasks keine Zugriffserlaubnis für den Speicherort hat. Es ist möglich, dass Sie für eine Netzwerkfreigabe oder ein Storage Node-Depot noch weitere Anmeldedaten brauchen.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
2. Klicken Sie auf **OK**.

Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

5.1.3 Anmeldedaten für das Ziel

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Anmeldedaten des Tasks benutzen**

     Das Programm greift auf den Zielort mit den Anmeldedaten des Task-Kontos zu, wie sie im Abschnitt **Task-Parameter** spezifiziert wurden.
   - **Folgende Anmeldedaten verwenden**

     Das Programm greift auf den Zielort unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu. Verwenden Sie diese Option, sofern das Konto des Tasks keine Zugriffserlaubnis für den Zielort hat.

Spezifizieren Sie:

- **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
- **Kennwort**. Das Kennwort für das Konto.

2. Klicken Sie auf **OK**.

5.1.4 Recovery-Ziel

Spezifizieren Sie das Ziel, auf dem die gewählten Daten wiederhergestellt werden sollen.

5.1.4.1 Ziellaufwerke wählen

Die als Ziel verfügbaren Laufwerke oder Volumes hängen davon ab, welcher Agent auf der Maschine arbeitet.

Recovery zu:

Physikalische Maschine

Ist verfügbar, wenn der Acronis Backup & Recovery 11.5 Agent für Windows oder Agent für Linux installiert ist.

Die gewählten Laufwerke werden zu den physikalischen Laufwerken der Maschine wiederhergestellt, mit der die Konsole verbunden ist. Auf diese Auswahl hin fahren Sie dann mit der nachfolgend beschriebenen, regulären Laufwerk-Mapping-Prozedur fort.

Neue virtuelle Maschine

- *Falls der Acronis Backup & Recovery 11.5 Agent für Windows oder der Agent für Linux installiert ist.*

  Die ausgewählten Laufwerke werden zu einer neuen virtuellen Maschine wiederhergestellt, die einem der folgenden Typen entspricht: VMware Workstation, Microsoft Virtual PC, Red Hat Kernel-based Virtual Machine (KVM), Red Hat Enterprise Virtualization (RHEV) oder Citrix XenServer Open Virtual Appliance (OVA).

  Die Dateien der virtuellen Maschine werden zu dem Ziel gespeichert, welches Sie im Bereich **Storage** spezifizieren. Die neue virtuelle Maschine wird standardmäßig im persönlichen Ordner für Dokumente des aktuellen Benutzers erstellt.

- *Falls der Acronis Backup & Recovery 11.5 Agent für Hyper-V oder der Agent für ESX(i) installiert ist.*

  Diese Agenten ermöglichen es, eine neue virtuelle Maschine auf einem von Ihnen angegebenen Virtualisierungsserver zu erstellen.

  Die neue virtuelle Maschine wird standardmäßig im Standard-Storage des Virtualisierungsservers erstellt. Ob Sie den Speicherort auf dem Virtualisierungsserver verändern können oder nicht, hängt vom Fabrikat und den Einstellungen des Virtualisierungsprodukts ab. VMware ESX(i) kann mehrere Speicherorte haben. Ein Microsoft Hyper-V-Server ermöglicht das Erstellen einer neuen virtuellen Maschine in jedem lokalen Ordner.

Die neue virtuelle Maschine wird automatisch konfiguriert, sofern möglich wird die Konfiguration der Quellmaschine kopiert. Die Konfiguration wird im Abschnitt **Einstellungen der virtuellen Maschine** (S. 198) angezeigt. Überprüfen Sie die Einstellungen und führen Sie, sofern benötigt, Änderungen aus.

Dann fahren Sie mit der nachfolgend beschriebenen, regulären Laufwerk-Mapping-Prozedur fort.

Existierende virtuelle Maschine

Ist verfügbar, wenn der Acronis Backup & Recovery 11.5 Agent für Hyper-V oder der Agent für ESX(i) installiert ist.

Mit dieser Auswahl spezifizieren Sie den Virtualisierungsserver und die virtuelle Zielmaschine. Dann fahren Sie mit der nachfolgend beschriebenen, regulären Laufwerk-Mapping-Prozedur fort.

Beachten Sie, dass die Zielmaschine vor der Wiederherstellung automatisch ausgeschaltet wird. Modifizieren Sie die Option Zustand der VM steuern, falls Sie es vorziehen, diese manuell auszuschalten.

Laufwerke/Volumes

Automatisch zuordnen

Acronis Backup & Recovery 11.5 versucht die gewählten Laufwerke den entsprechenden Ziellaufwerken so zuzuordnen, wie im Abschnitt 'Wie die automatische Zuordnung arbeitet (S. 156)' beschrieben. Sollten Sie mit dem Zuordnungsergebnis unzufrieden sein, dann können Sie die Laufwerke manuell neu zuordnen. Dazu müssen Sie die Zuordnung der Laufwerke in umgekehrter Reihenfolge wieder aufheben, die Zuordnung des zuletzt zugeordneten Laufwerks sollte also zuerst aufgehoben werden. Führen Sie die manuelle Zuordnung der Laufwerke dann wie nachfolgend beschrieben durch.

Laufwerk Nr.:

Laufwerk Nr. (MODELL) (S. 155)

Bestimmten Sie für jedes Quelllaufwerk das entsprechende Ziellaufwerk.

NT-Signatur (S. 155)

Bestimmten Sie, auf welche Art die wiederhergestellte Disk-Signatur gehandhabt wird. Eine Disk-Signatur wird von Windows sowie Linux-Kernel Version 2.6 und später verwendet.

Zielfestplatte

So spezifizieren Sie ein Ziellaufwerk:

1. Bestimmen Sie eine Festplatte, wohin Sie die gewählte Festplatte wiederhergestellt haben wollen. Der Platz der Zielfestplatte sollte mindestens die Größe der unkomprimierten Daten des Images haben.
2. Klicken Sie auf **OK**.

Alle auf der Zielfestplatte gespeicherten Daten werden durch die im Backup befindlichen Daten ersetzt, seien Sie also vorsichtig und achten Sie auf noch nicht gesicherte Daten, die noch benötigt werden.

NT-Signatur

Die NT-Signatur ist ein spezieller Datensatz, die im MBR hinterlegt ist. Sie dient der eindeutigen Identifizierung eines Laufwerks für das Betriebssystem.

Bei Wiederherstellung eines Laufwerks mit einem System-Volume können Sie wählen, was mit der NT-Signatur des Ziellaufwerks gemacht werden soll. Spezifizieren Sie einen der folgenden Parameter:

- **Automatische Auswahl**

  Die Software bewahrt die NT-Signatur des Ziellaufwerks, falls es sich um dieselbe NT-Signatur wie die im Backup vorliegende handelt. (Also mit anderen Worten, wenn Sie das Laufwerk auf dasselbe Laufwerk wiederherstellen, das zuvor ins Backup gesichert wurde). Anderenfalls generiert die Software eine neue NT-Signatur für das Ziellaufwerk.

  Diese vorgegebene Auswahl wird für die meisten Fälle empfohlen. Verwenden Sie die folgenden Einstellungen nur, wenn Sie sie wirklich benötigen.

- **Neu erstellen**

  Acronis Backup & Recovery 11.5 generiert eine neue NT-Signatur für das Ziellaufwerk.

- **Aus dem Backup wiederherstellen**

  Acronis Backup & Recovery 11.5 wird die NT-Signatur des Ziellaufwerks mit derjenigen aus dem Laufwerk-Backup ersetzen.

  ***Anmerkung**: Sie sollten sich absolut sicher sein, dass keine der in dieser Maschine vorhandenen Laufwerke dieselbe NT-Signatur hat. Anderenfalls startet das Betriebssystem vom ersten Laufwerk, erkennt dabei die gleiche Signatur auf dem zweiten Laufwerk, erzeugt automatisch eine neue, eindeutige NT-Signatur und weist diese dem zweiten Laufwerk zu. Als Konsequenz verlieren darauf dann alle Volumes des zweiten Laufwerks ihre Laufwerksbuchstaben, werden Verzeichnispfade ungültig und können Programme ihre Dateien nicht mehr finden. Das Betriebssystem auf diesem Laufwerk kann daher auch nicht mehr booten.*

  Eine Wiederherstellung der Disk-Signatur kann aus folgenden Gründen wünschenswert sein:

  - Acronis Backup & Recovery 11.5 steuert die Planung von Tasks unter Verwendung der Signatur des Quelllaufwerks. Wenn Sie dieselbe Disk-Signatur wiederherstellen, müssen Sie bereits erzeugte Tasks nicht neu erstellen oder bearbeiten.
  - Einige installierte Anwendungen verwenden eine Disk-Signatur zur Lizenzierung oder für andere Einsatzzwecke.
  - Das ermöglicht es Ihnen, alle Systemwiederherstellungspunkte von Windows auf dem wiederhergestellten Laufwerk zu behalten.
  - So stellen Sie VSS-Snapshots (VSS = virtueller Schattenkopie-Dienst) wieder her, die von der Windows Vista-Funktion 'Vorherige Versionen' verwendet werden.

- **Existierende erhalten**

  Das Programm lässt die NT-Signatur des Ziellaufwerks unberührt.

Wie die automatische Zuordnung arbeitet

Acronis Backup & Recovery 11.5 führt nur dann eine automatische Zuordnung der Laufwerke bzw. Volumes zu den Ziellaufwerken durch, wenn dabei die Bootfähigkeit des Systems bewahrt wird. Anderenfalls wird die automatische Zuordnung abgebrochen und Sie müssen die Laufwerke bzw. Volumes automatisch zuordnen.

Sie müssen die Volumes außerdem auch dann manuell zuordnen, wenn logische Linux-Volumes oder Linux Software RAID-Volumes (MD-Geräte) vorliegen. Zu weiteren Informationen über die Wiederherstellung von logischen Volumes und MD-Geräten siehe den Abschnitt 'MD-Gerдte und logische Volumes wiederherstellen (S. 48)'

Die automatische Zuordnung (Mapping) läuft folgendermaßen ab.

1. Wenn ein Laufwerk oder Volume zu seinem ursprünglichen Speicherort wiederhergestellt wird, dann reproduziert der Zuordnungsprozess das ursprüngliche Laufwerks- bzw. Volume-Layout.

   Der 'ursprüngliche' Speicherort für das Laufwerk bzw. Volume bedeutet, dass es sich um exakt dasselbe Laufwerk oder Volume handeln muss, das per Backup gesichert wurde. Ein Volume wird nicht als 'ursprünglich' betrachtet, wenn es seit dem Backup hinsichtlich Größe, Speicherort oder anderen physikalischen Parametern geändert wurde. Änderungen beim Laufwerksbuchstaben oder der Bezeichnung hindern die Software jedoch nicht daran, das Volume korrekt zu erkennen.

2. Falls das Laufwerk oder Volume zu einem anderen Speicherort wiederhergestellt wird:
   - **Bei Wiederherstellung von Laufwerken**: Die Software überprüft die Ziellaufwerke auf Größe und Volumes. Ein Ziellaufwerk darf keine Volumes enthalten und seine Größe muss ausreichend sein, um das wiederherzustellende Laufwerk aufzunehmen. Noch nicht initialisierte Ziellaufwerke werden automatisch initialisiert.

Falls die benötigten Laufwerke nicht gefunden werden können, müssen Sie die Laufwerke manuell zuordnen.

- **Bei Wiederherstellung von Volumes**: Die Software überprüft die Ziellaufwerke auf 'nicht zugeordneten' Speicherplatz.

  Falls der 'nicht zugeordnete' Speicherplatz ausreicht, werden die Volumes 'wie vorliegend' wiederhergestellt.

  Falls der 'nicht zugeordnete' Speicherplatz auf den Ziellaufwerken kleiner als die Größe der wiederherzustellenden Volumes ist, dann werden die Volumes proportional so angepasst (durch Verringerung ihres freien Speicherplatzes), dass Sie auf den 'nicht zugeordneten' Speicherplatz passen. Falls die verkleinerten Volumes immer noch nicht auf den 'nicht zugeordneten' Speicherplatz passen, müssen Sie die Volumes manuell zuordnen.

Unterstützung für Festplatten mit Advanced Format (4K-Sektoren)

Acronis Backup & Recovery 11.5 kann sowohl Backups von Festplatten mit einer Sektorgröße von 4 KB erstellen (auch bekannt als Advanced Format-Laufwerke), wie auch von herkömmlichen Festplatten, die 512-Byte-Sektoren haben.

Acronis Backup & Recovery 11.5 kann Daten von einem dieser Laufwerke zu einem anderen wiederherstellen, solange *beide Laufwerke dieselbe logische Sektorgröße haben*. (Dies ist die gegenüber dem Betriebssystem präsentierte Sektorgröße.) Acronis Backup & Recovery 11.5 führt automatisch ein Alignment der Laufwerks-Volumes (S. 161) aus, sofern dies erforderlich ist. Auf diese Weise stimmt der Start eines Clusters im Dateisystem immer mit dem Start eines physikalischen Sektors auf dem Laufwerk überein.

Die Funktionalität zur Laufwerksverwaltungs (S. 300) von Acronis Backup & Recovery 11.5 steht für Laufwerke mit einer logischen Sektorgröße von 4-KB nicht zur Verfügung.

Bestimmung der logischen Sektorgröße

Anhand der Laufwerksspezifikation

Die Entwicklung der Advanced Format-Technologie wird von der 'International Disk Drive Equipment and Materials Association' (IDEMA) koordiniert. Weitere Details finden Sie unter http://www.idema.org/?page_id=2.

In Bezug auf die logische Sektorgröße spezifiziert die IDEMA zwei Typen von Advanced Format-Laufwerken:

- Laufwerke mit **512 Byte-Emulation (512e)** haben eine logische Sektorgröße von 512 Byte. Diese Laufwerke werden von Windows beginnend mit Windows Vista und von modernen Linux-Distributionen unterstützt. Microsoft und Western Digital verwenden den Ausdruck 'Advanced Format' exklusiv nur für diesen Laufwerkstyp.
- Laufwerke vom Typ **4K nativ (4Kn)** haben eine logische Sektorgröße von 4-KByte. Moderne Betriebssystem können Daten auf solchen Laufwerken speichern, meistens aber nicht von ihnen booten. Solche Laufwerken sind üblicherweise externe Laufwerke mit USB-Verbindung.

Durch Ausführung eines entsprechenden Befehls

Gehen Sie folgendermaßen vor, um die logische Sektorgröße eines Laufwerks zu ermitteln.

In Windows:

1. Stellen Sie sicher, dass das Laufwerk ein NTFS-Volume enthält.

2. Führen Sie folgenden Befehl als Administrator aus, unter Angabe des Laufwerksbuchstaben für das NTFS-Volume:

```
fsutil fsinfo ntfsinfo D:
```

3. Bestimmen Sie den Wert in der Zeile **Bytes pro Sektor**. Die Ausgabe kann beispielsweise wie folgt aussehen:

```
Bytes pro Sektor: 512
```

In Linux:

1. Ermitteln Sie den Gerätenamen des Laufwerks, wie etwa /dev/sdb.
2. Führen Sie folgenden Befehl als Benutzer 'root' aus, unter Angabe des Gerätenamens:

```
parted /dev/sdb print
```

3. Bestimmen Sie den ersten Wert in der Zeile **Sektorgröße (logisch/physisch)**. Die Ausgabe kann beispielsweise wie folgt aussehen:

```
Sektorgröße (logisch/physisch): 512B/4096B
```

5.1.4.2 Ziel-Volumes wählen

Die verfügbaren Ziele für Volumes hängen davon ab, welcher Agent auf der Maschine arbeitet.

Recovery zu:

Physikalische Maschine

Ist verfügbar, wenn der Acronis Backup & Recovery 11.5 Agent für Windows oder Agent für Linux installiert ist.

Die gewählten Volumes (Partitionen) werden zu den physikalischen Laufwerken der Maschine wiederhergestellt, mit der die Konsole verbunden ist. Auf diese Auswahl hin fahren Sie dann mit der nachfolgend beschriebenen, regulären Laufwerk-Mapping-Prozedur fort.

Neue virtuelle Maschine

- *Falls der Acronis Backup & Recovery 11.5 Agent für Windows oder der Agent für Linux installiert ist.*

  Die ausgewählten Volumes werden zu einer neuen virtuellen Maschine wiederhergestellt, die einem der folgenden Typen entspricht: VMware Workstation, Microsoft Virtual PC, Red Hat Kernel-based Virtual Machine (KVM), Red Hat Enterprise Virtualization (RHEV) oder Citrix XenServer Open Virtual Appliance (OVA).

  Die Dateien der virtuellen Maschine werden zu dem Ziel gespeichert, welches Sie im Bereich **Storage** spezifizieren. Die neue virtuelle Maschine wird standardmäßig im persönlichen Ordner für Dokumente des aktuellen Benutzers erstellt.

- *Falls der Acronis Backup & Recovery 11.5 Agent für Hyper-V oder der Agent für ESX(i) installiert ist.*

  Diese Agenten ermöglichen es, eine neue virtuelle Maschine auf einem von Ihnen angegebenen Virtualisierungsserver zu erstellen.

  Die neue virtuelle Maschine wird standardmäßig im Standard-Storage des Virtualisierungsservers erstellt. Ob Sie den Speicherort auf dem Virtualisierungsserver verändern können oder nicht, hängt vom Fabrikat und den Einstellungen des Virtualisierungsprodukts ab. VMware ESX(i) kann mehrere Speicherorte haben. Ein Microsoft Hyper-V-Server ermöglicht das Erstellen einer neuen virtuellen Maschine in jedem lokalen Ordner.

Die neue virtuelle Maschine wird automatisch konfiguriert, sofern möglich wird die Konfiguration der Quellmaschine kopiert. Die Konfiguration wird im Abschnitt **Einstellungen der virtuellen Maschine**

(S. 198) angezeigt. Überprüfen Sie die Einstellungen und führen Sie, sofern benötigt, Änderungen aus.

Dann fahren Sie mit der nachfolgend beschriebenen, regulären Laufwerk-Mapping-Prozedur fort.

Existierende virtuelle Maschine

Ist verfügbar, wenn der Acronis Backup & Recovery 11.5 Agent für Hyper-V oder der Agent für ESX(i) installiert ist.

Mit dieser Auswahl spezifizieren Sie den Virtualisierungsserver und die virtuelle Zielmaschine. Dann fahren Sie mit der nachfolgend beschriebenen, regulären Laufwerk-Mapping-Prozedur fort.

Beachten Sie, dass die Zielmaschine vor der Wiederherstellung automatisch ausgeschaltet wird. Modifizieren Sie die Option Zustand der VM steuern, falls Sie es vorziehen, diese manuell auszuschalten.

Laufwerke/Volumes

Automatisch zuordnen

Acronis Backup & Recovery 11.5 versucht die gewählten Volumes den entsprechenden Ziellaufwerken so zuzuordnen, wie im Abschnitt 'Wie die automatische Zuordnung arbeitet (S. 156)' beschrieben. Sollten Sie mit dem Zuordnungsergebnis unzufrieden sein, dann können Sie die Volumes manuell neu zuordnen. Dazu müssen Sie die Zuordnung der Volumes in umgekehrter Reihenfolge wieder aufheben, die Zuordnung des zuletzt zugeordneten Volumes sollte also zuerst aufgehoben werden. Führen Sie die manuelle Zuordnung der Volumes dann wie nachfolgend beschrieben durch.

[Disk Nr.] MBR wiederherstellen auf: [wenn der Master Boot Record für die Wiederherstellung ausgewählt ist]

Laufwerk Nr. (S. 159)

Wählen Sie das Laufwerk, auf der der Master Boot Record wiederhergestellt wird.

NT-Signatur: (S. 155)

Bestimmen Sie, wie die Laufwerk-Signatur im MBR gehandhabt wird. Eine Disk-Signatur wird von Windows sowie Linux-Kernel Version 2.6 und später verwendet.

[Laufwerk] [Buchstabe] wiederherstellen auf:

Laufwerk Nr. /Volume

Ordnen Sie nacheinander jedem Quell-Volume einem Volume des Ziellaufwerkes oder 'nicht zugeordnetem' Speicherplatz zu.

Größe: (S. 160)

[Optional] Ändern Sie Größe, Position oder andere Eigenschaften des wiederhergestellten Volumes.

MBR-Ziel

So spezifizieren Sie ein Ziellaufwerk:

1. Wählen Sie das Ziellaufwerk aus, auf dem Sie den MBR wiederherstellen möchten.
2. Klicken Sie auf **OK**.

Ziel für ein Volume

So spezifizieren Sie ein Ziel-Volume oder 'nicht zugeordneten' Speicherplatz

1. Bestimmen Sie ein Volume oder 'nicht zugeordneten' Speicherplatz, wohin Sie das gewählte Volume wiederherstellen wollen. Das Ziel-Volume bzw. der nicht zugeordnete Speicherplatz sollten mindestens die Größe der unkomprimierten Daten des Images haben.
2. Klicken Sie auf **OK**.

Alle auf dem Ziel-Volume gespeicherten Daten werden durch die im Backup befindlichen Daten ersetzt, seien Sie also vorsichtig und achten Sie auf noch nicht gesicherte Daten, die noch benötigt werden.

Bei Verwendung bootfähiger Medien

Laufwerksbuchstaben, die unter Windows-basierten Boot-Medien zu sehen sind, können von der Art abweichen, wie Windows seine Laufwerke normalerweise identifiziert. So könnte beispielsweise die Zuordnung des Laufwerks D: unter dem Rettungs-Utility dem Laufwerk E: entsprechen, welches Windows verwendet.

Achtung! Um auf der sicheren Seite zu sein, ist es ratsam, den jeweils verwendeten Volumes eindeutige Namen zuzuweisen.

Ein Linux-typisches bootfähiges Medium zeigt lokale Laufwerke und Volumes als 'unmounted' an (sda1, sda2...).

Volume-Eigenschaften ändern

Größe und Speicherort

Sie können bei Wiederherstellung eines Volumes auf ein Basis-Laufwerk vom Typ MBR das Volume in seiner Größe oder Lage verändern, indem Sie dessen Darstellung bzw. Ränder mit der Maus verschieben oder indem Sie korrespondierende Werte in die entsprechenden Felder eingeben. Durch Verwendung dieser Funktion können Sie den Speicherplatz zwischen den wiederherzustellenden Volumes aufteilen. In diesem Fall müssen Sie zuerst das Volume wiederherstellen, welches in seiner Größe reduziert werden soll.

***Beachten Sie:** Volumes, die mit der Option 'Sektor-für-Sektor' gesichert wurden, können nicht in der Größe angepasst werden.*

***Tipp:** Die Größe eines Volumes kann nicht verändert werden, wenn es aus einem Backup wiederhergestellt wird, das auf mehrere entfernbare Medien verteilt wurde. Um die Größe des Volumes zu ändern, kopieren Sie alle Teile des Backups an einen einzigen Speicherort auf einer Festplatte (oder ähnlichem Laufwerk).*

Typ

Ein Basis-Laufwerk vom Typ MBR kann bis zu vier primäre Volumes enthalten – oder bis zu drei primäre Volumes sowie ein bis mehrere logische Laufwerke. Das Programm wählt standardmäßig den ursprünglichen Typ des Volumes. Sie können diese Einstellung ändern (falls erforderlich).

- **Primär**. Die Informationen über primäre Volumes sind in der MBR-Partitionstabelle enthalten. Die meisten Betriebssysteme können nur von einem primären Volume auf dem ersten Laufwerk booten, zudem ist die Zahl primärer Volumes limitiert.

  Wählen Sie bei Wiederherstellung eines System-Volumes auf ein Basis-Laufwerk vom Typ MBR das Kontrollkästchen 'Aktiv'. Ein aktives Volume wird zum Starten eines Betriebssystems verwendet. Wenn Sie jedoch 'Aktiv' für ein Volume ohne installiertes Betriebssystem wählen, kann das die Maschine daran hindern, zu booten. Ein logisches Laufwerk oder ein dynamisches Volume kann nicht auf 'Aktiv' gesetzt werden.

- **Logisch**. Die Informationen über logische Volumes sind nicht im MBR, sondern in der erweiterten Partitionstabelle hinterlegt. Die Anzahl logischer Volumes auf einer Festplatte (oder ähnlichem Laufwerk) ist nicht limitiert. Ein logisches Volume kann nicht als 'Aktiv' gesetzt werden. Wenn Sie ein System-Volume auf ein anderes Laufwerk mit eigenen Volumes (Partitionen) und Betriebssystem wiederherstellen, benötigen Sie wahrscheinlich nur die entsprechenden Daten. In diesem Fall können Sie das Volume auch als logisches Laufwerk wiederherstellen, um lediglich auf seine Daten zuzugreifen.

Dateisystem

Standardmäßig erhalten wiederhergestellte Volumes dasselbe Dateisystem wie das ursprünglich gesicherte Volume. Falls benötigt, können Sie jedoch das Dateisystem des Volumes während der Recovery-Aktion ändern.

Acronis Backup & Recovery 11.5 kann folgende Dateisysteme zueinander konvertieren: FAT16 –> FAT32 und Ext2 –> Ext3. Für Volumes mit anderen nativen Dateisystemen ist diese Option nicht verfügbar.

Angenommen, Sie wollen ein Volume von einem alten FAT16-Laufwerk mit niedriger Kapazität auf einer neueren Festplatte wiederherstellen. FAT16 wäre nicht effektiv und es könnte unter Umständen auch unmöglich sein, dieses Dateisystem auf das neue Laufwerk zu übertragen. Hintergrund ist, dass FAT16 nur Volumes bis 4 GB unterstützt, daher können Sie ein 4 GB FAT16-Volume nicht ohne Änderung des Dateisystems auf ein Laufwerk wiederherstellen, welches über dieser Begrenzung liegt. In diesem Fall wäre es sinnvoll, das Dateisystem von FAT16 zu FAT32 zu wechseln.

Ältere Betriebssysteme (MS-DOS, Windows 95 und Windows NT 3.x, 4.x) unterstützen jedoch kein FAT32 und sind daher nicht betriebsbereit, nachdem Sie das Volume wiederhergestellt und das Dateisystem geändert haben. Diese können normalerweise nur auf ein FAT16-Volume wiederhergestellt werden.

Alignment von Volumes (Partitionen)

Acronis Backup & Recovery 11.5 beseitigt die Fehlausrichtung (Misalignment) von Volumes automatisch – also Situationen, in denen Volume-Cluster nicht passend zu den Laufwerkssektoren ausgerichtet sind. Zu einem Misalignment kommt es, wenn ein Volume, das mit einem CHS-Adressschema (Cylinder/Head/Sector) erstellt wurde, auf ein Laufwerk (Festplatte oder SSD) wiederhergestellt wird, welches eine Sektorgröße von 4 KB nutzt. Das CHS-Adressschema wird beispielsweise von allen Windows-Betriebssystemen vor Windows Vista verwendet.

Wenn bei Volumes ein Misalignment vorliegt, überlappen die Cluster mehr physikalische Sektoren, als es bei korrektem Alignment der Fall wäre. Als Folge müssen bei jeder Datenänderung mehr physikalische Sektoren als eigentlich nötig gelöscht und überschrieben werden. Diese unnötigen Lese-/Schreib-Operationen verringern spürbar die Laufwerksgeschwindigkeit (und damit auch die Gesamt-Performance des Systems). Ein Misalignment bei SSDs (Solid State Drives) verringert nicht nur die Performance des Systems bzw. Laufwerks, sondern auch dessen Lebensdauer. Da die Speicherzellen von SSDs nur auf eine bestimmte Menge von Lese-/Schreib-Operationen ausgelegt sind, führen redundante Lese-/Schreib-Operationen daher zu einem vorschnellen Verschleiß des SSD-Laufwerks.

Bei der Wiederherstellung von dynamischen Volumes und von logischen Volumes, die unter Linux mit dem Logical Volume Manager (LVM) erstellt wurden, wird das passende Alignment automatisch eingestellt.

Bei der Wiederherstellung von Basis-Volumes des Typs 'MBR' und 'GPT' können Sie die Alignment-Methode manuell wählen, sofern Sie das automatische Alignment aus irgendwelchen Gründen nicht zufriedenstellt. Folgende Optionen sind verfügbar:

- **Automatische Auswahl** – (Standard) empfohlen. Die Software stellt das passende Alignment automatisch ein, basierend auf den Laufwerk- bzw. Volume-Eigenschaften von Quelle und Ziel.

  Verwenden Sie die folgenden Optionen nur, wenn Sie sie wirklich benötigen.
  - **CHS (63 Sektoren)** – wählen Sie diese Option, wenn das wiederherzustellende Volume unter Windows XP oder Windows Server 2003 (oder früher) mit Laufwerken verwendet werden soll, die 512 Byte pro physikalischen Sektor haben.
  - **VMware VMFS (64 KB)** – wählen Sie diese Option, wenn Sie das Volume als eine 'VMware Virtual Machine File System'-Partition wiederherstellen wollen.
  - **Vista-Alignment (1 MB)** – wählen Sie diese Option, wenn das wiederherzustellende Volume unter Windows-Betriebssystemen ab Windows Vista (aufwärts) verwendet werden soll – oder wenn Sie das Volume auf ein Festplatten- oder SSD-Laufwerk wiederherstellen wollen, das eine Sektorgröße von 4 KB hat.
  - **Benutzerdefiniert** – spezifizieren Sie das Volume-Alignment manuell. Es wird empfohlen, dass der Wert ein Vielfaches der physikalischen Sektorgröße ist.

Logische Laufwerksbuchstaben (nur für Windows)

Standardmäßig wird dem Volume der erste freie Buchstabe zugewiesen. Wenn Sie einen anderen Laufwerksbuchstaben zuweisen wollen, dann wählen Sie einen entsprechenden aus dem Listenfeld.

Falls Sie den leeren Eintrag wählen, wird dem wiederhergestellten Volume kein Laufwerksbuchstabe zugewiesen und es so vor dem Betriebssystem verborgen. Sie sollten keine Laufwerksbuchstaben für Volumes vergeben, auf die Windows nicht zugreifen kann, beispielsweise bei Volumes, die kein FAT oder NTFS als Dateisystem verwenden.

5.1.4.3 Zielspeicherort für Dateien und Ordner wählen

Recovery-Ziel

Ziel

Wählen Sie einen Speicherort, in den die gesicherten Dateien wiederhergestellt werden:

- **Ursprünglicher Speicherort**

  Die Dateien und Ordner werden zu demselben Pfad(en) wiederhergestellt, wie sie im Backup vorliegen. Falls Sie z.B. alle Dateien und Ordner aus *C:\Dokumente\Finanzen\Berichte* gesichert hatten, so werden die Daten zu genau diesem Pfad wiederhergestellt. Sollte der Ordner nicht existieren, dann wird er automatisch erstellt.
- **Neuer Speicherort**

  Die Dateien werden zu dem Speicherort wiederhergestellt, den Sie im Verzeichnisbaum spezifizieren. Dabei werden die Dateien und Ordner ohne Anlegen eines vollständigen Pfades zurückgesichert, es sei denn, Sie deaktivieren das Kontrollkästchen **Ohne absolute Pfade wiederherstellen**.

Überschreiben

Bestimmen Sie, was geschehen soll, wenn das Programm im Zielordner eine Datei gleichen Namens wie im Archiv findet:

- **Existierende Dateien überschreiben** – dies gibt der Datei im Backup eine höhere Priorität als der Datei auf dem Ziellaufwerk.

- **Existierende Datei überschreiben, wenn sie älter ist** – Dateien mit den jüngsten Veränderungen erhalten Priorität, egal ob sie im Backup oder auf dem Laufwerk sind.
- **Existierende Dateien nicht überschreiben** – dies gibt der Datei auf dem Ziellaufwerk eine höhere Priorität als der Datei im Backup.

Falls Sie ein Überschreiben von Dateien erlauben, haben Sie dennoch die Option, spezielle Dateien davor zu schützen, nämlich indem Sie diese von der Recovery-Aktion ausschließen.

Ausschließungen vom Recovery (S. 163)

Spezifizieren Sie die Dateien und Ordner, die nicht wiederhergestellt werden sollen.

Ausschließungen vom Recovery

Richten Sie Ausschlusskriterien für spezielle Dateien und Ordner ein, die sie nicht wiederherstellen wollen.

***Hinweis:** Ausschließungen überschreiben eine Auswahl von wiederherzustellenden Datenelementen. Falls Sie beispielsweise festlegen, dass die Datei 'MeineDatei.tmp' wiederhergestellt werden soll und Sie aber zudem alle .tmp-Dateien ausschließen, dann wird 'MeineDatei.tmp' nicht wiederhergestellt.*

Verwenden Sie die Schaltflächen **Hinzufügen**, **Bearbeiten**, **Entfernen** und **Alle entfernen**, um die Liste der auszuschließenden Dateien und Ordner zu verwalten. Spezifizieren Sie den Namen der Datei oder des Ordners, wie etwa 'Dokument.txt'.

Bei den Namen wird *nicht* auf Groß-/Kleinschreibung geachtet (in Windows und Linux). Falls Sie beispielsweise festlegen, dass alle .tmp-Dateien und Temp-Ordner ausgeschlossen werden sollen, dann werden auch alle .Tmp-Dateien, alle .TMP-Dateien und alle TEMP-Ordner ausgeschlossen.

Sie können ein oder mehrere Platzhalterzeichen (* und ?) verwenden:

- Das Asterisk (*) ersetzt null bis mehrere Zeichen. So beinhaltet beispielsweise 'Doc*.txt' Dateien wie 'Doc.txt' und 'Document.txt'.
- Das Fragezeichen (?) steht für exakt ein Zeichen. Beispielsweise beinhaltet 'Doc?.txt' Dateien wie 'Doc1.txt' und 'Docs.txt' – aber nicht 'Doc.txt' oder 'Doc11.txt'.

Beispiele für Ausschließungen

Kriterium	Beispiel	Beschreibung
Per Name	F.log F	Schließt alle Dateien namens 'F.log' aus Schließt alle Ordner namens 'F' aus
Per Maske (*)	*.log F*	Schließt alle Dateien mit der Erweiterung „.log“ aus Schließt alle Dateien und Ordner aus, deren Namen mit „F“ beginnen (etwa die Ordner F, F1 und die Dateien F.log, F1.log)
Per Maske (?)	F???.log	Schließt alle .log-Dateien aus, deren Namen am Ende vier Zeichen enthalten und mit „F“ beginnen

5.1.5 Recovery-Zeitpunkt

Bestimmen Sie, wann der Recovery-Task beginnen soll:

- **Jetzt** – der Recovery-Task wird direkt gestartet, sobald Sie auf der Seite **Daten wiederherstellen** auf **OK** klicken.

- **Später** – der Recovery-Tasks wird später manuell gestartet. Falls Sie eine Planung für den Task erstellen müssen, dann deaktivieren Sie das Kontrollkästchen **Task wird manuell gestartet** und spezifizieren Sie den gewünschten Zeitpunkt.

5.1.6 Anmeldedaten für den Task

Stellen Sie die Anmeldedaten für das Konto zur Verfügung, mit dem der Task ausgeführt wird.

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Unter dem aktuellen Benutzer ausführen**

     Der Task wird mit den Anmeldedaten des Benutzers ausgeführt, der die Tasks startet. Wenn der Task nach Zeit-/Ereignis-Planung laufen soll, werden Sie bei Abschluss der Task-Erstellung nach dem Passwort des aktuellen Benutzers gefragt.
   - **Folgende Anmeldedaten verwenden**

     Der Task wird immer mit den von Ihnen spezifizierten Anmeldedaten ausgeführt, egal ob manuell oder per Zeit-/Ereignis-Planung gestartet.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
2. Klicken Sie auf 'OK'.

Weitere Informationen über die Verwendung von Anmeldedaten in Acronis Backup & Recovery 11.5 finden Sie im Abschnitt 'In Backup-Plänen und Tasks verwendete Anmeldedaten (S. 35)'.

Siehe den Abschnitt 'Benutzerberechtigungen auf einer verwalteten Maschine (S. 37)', um mehr über Aktionen zu erfahren, die in Abhängigkeit von Benutzerberechtigungen verfügbar sind.

5.2 Acronis Universal Restore

Acronis Universal Restore ist eine proprietäre Acronis-Technologie, die Ihnen hilft, ein Betriebssystem auf abweichender Hardware oder einer virtuellen Maschine wiederherzustellen und zu booten. Universal Restore handhabt Abweichungen bei Geräten, die kritisch für den Betriebssystemstart sind, wie beispielsweise Speicher-Controller, Hauptplatine oder Chipsatz.

Universal Restore ist bei folgenden Szenarien besonders nützlich:

1. Sofortige Wiederherstellung eines ausgefallenen Systems auf abweichender Hardware.
2. Hardware-unabhängiges Klonen und Deployment von Betriebssystemen.
3. Migration von Maschinen von physikalisch zu physikalisch, physikalisch zu virtuell und virtuell zu physikalisch.

5.2.1 Universal Restore erwerben

Universal Restore ist immer verfügbar, wenn Sie ein System aus dem Online Storage wiederherstellen.

Universal Restore ist kostenlos in der Acronis Backup & Recovery 11.5 Advanced Server SBS Edition und der Virtual Edition enthalten.

Für die anderen Produkt-Editionen muss Universal Restore separat erworben werden. Es hat seine eigene Lizenz.

Wählen Sie zur Aktivierung von Universal Restore eine der folgenden Möglichkeiten:

- Installieren Sie Universal Restore aus dem Installationspaket des Produktes (zusätzlich zum Agenten für Windows, Agenten für Linux oder dem Bootable Media Builder).
- Falls der Agent bereits installiert sein sollte, können Sie die Management Konsole mit der Maschine verbinden, auf **Hilfe –> Lizenz wechseln** klicken und dann den Lizenzschlüssel oder den License Server spezifizieren, von wo die Universal Restore-Lizenz genommen werden soll.

Sie müssen neue bootfähige Medien erstellen, um das neu installierte Add-on auch in der bootfähigen Umgebung einsetzbar zu machen.

5.2.2 Universal Restore verwenden

Während einer Wiederherstellung

Universal Restore ist verfügbar, wenn Sie ein Laufwerk oder Volume wiederherstellen und dabei ein Windows- oder Linux-Betriebssystem in der Auswahl Ihrer Laufwerke bzw. Volumes enthalten ist. Sollte Ihre Auswahl mehr als ein Betriebssystem beinhalten, können Sie Universal Restore entweder auf alle Windows-Systeme, alle Linux-Systeme oder beide Systeme zusammen anwenden.

Falls die Software nicht erkennen kann, ob in dem Backup ein Betriebssystem vorhanden ist, schlägt sie die Verwendung von Universal Restore aufs Geratewohl für den Fall vor, dass ein System vorhanden ist. Diese Fälle sind wie folgt:

- Das Backup ist in mehrere Dateien aufgeteilt
- Das Backup befindet sich in einem deduplizierenden Depot, auf dem Acronis Online Backup Storage, auf einem FTP-/SFTP-Server, auf Band, CD oder DVD.

Manchmal wird Universal Restore im Hintergrund angewendet, weil die Software weiß, welche Treiber oder Module für die unterstützte virtuelle Maschine benötigt werden. Diese Fälle sind wie folgt:

- Wiederherstellung eines Systems zu einer neuen virtuellen Maschine
- Wiederherstellung eines Systems zu einer virtuellen Maschine mittels eines Agenten für ESX(i) oder Agenten für Hyper-V.

Universal Restore ist nicht verfügbar, wenn:

- das Backup in der Acronis Secure Zone liegt
- Sie die Verwendung von Acronis Active Restore (S. 484) gewählt haben,

Und zwar weil alle diese Funktionen in erster Linie zur sofortigen Datenwiederherstellung auf der gleichen Maschine gedacht sind.

Ohne Wiederherstellung

Sie können Universal Restore auch unter einem bootfähigen Medium ohne Recovery-Aktion verwenden, indem Sie in der Willkommenseite des Mediums auf den Befehl **Universal Restore anwenden** klicken. Universal Restore wird auf das Betriebssystem angewendet, das bereits auf der Maschine existiert. Falls es mehrere Betriebssysteme gibt, werden Sie aufgefordert, dasjenige zu wählen, auf das Universal Restore angewendet werden soll.

5.2.2.1 Universal Restore in Windows

Vorbereitung

Treiber vorbereiten

Bevor Sie Universal Restore auf ein Windows-Betriebssystem anwenden, sollten Sie sicherstellen, dass Sie für den neuen Festplatten-Controller und Chipsatz die passenden Treiber haben. Diese Treiber sind für den Start des Betriebssystems entscheidend. Verwenden Sie die vom Hardware-Hersteller mitgelieferte CD bzw. DVD oder laden Sie die Treiber von der Website des Herstellers herunter. Die Treiber sollten die Erweiterungen *.inf, *.sys oder *.oem haben. Wenn Sie die Treiber im Format *.exe, *.cab oder *.zip herunterladen, dann extrahieren Sie diese unter Verwendung einer Dritthersteller-Anwendung.

Ein optimaler Ansatz ist es, die Treiber für die in Ihrer Organisation verwendete Hardware an einem Aufbewahrungsort zu speichern, sortiert nach Gerätetyp oder Hardware-Konfiguration. Sie können eine Kopie des Aufbewahrungsortes auf einer DVD oder einem USB-Stick vorhalten; verwenden Sie einige Treiber und fügen Sie diese den bootfähigen Medien hinzu; erstellen Sie für jeden Ihrer Server ein benutzerdefiniertes bootfähiges Medium mit den notwendigen Treibern (und der notwendigen Netzwerk-Konfiguration). Alternativ können Sie auch einfach jedes Mal, wenn Universal Restore verwendet wird, den Pfad zum Aufbewahrungsort angeben.

Überprüfen Sie den Zugriff auf die Treiber innerhalb der bootfähigen Notfallumgebung.

Stellen Sie sicher, dass Sie bei Verwendung eines bootfähigen Mediums auf das Gerät mit den Treibern zugreifen können. Sogar, wenn Sie eine Wiederherstellung des Systemlaufwerks unter Windows konfigurieren, wird die Maschine neu gestartet und die Recovery-Aktion dann in einer Linux-basierten Umgebung durchgeführt. Verwenden Sie ein WinPE-basiertes Medium, falls das Gerät unter Windows verfügbar ist, aber von einem Linux-basierten Notfallmedium nicht erkannt wird.

Was, wenn Sie keine Treiber haben?

Windows 7 enthält mehr Treiber als die früheren Windows-Betriebssysteme. Es besteht daher eine gute Chance, dass Universal Restore alle benötigten Treiber im Treiberordner von Windows 7 findet. Sie müssen also nicht unbedingt externe Pfade zu den Treibern angeben. Nichtsdestotrotz ist die Durchführung von Universal Restore kritisch, so dass das System die korrekten Treiber verwenden sollte.

*Der Standardordner von Windows zum Speichern von Treibern ist im Registry-Wert **DevicePath** hinterlegt, der im Registry-Schlüssel **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion** gefunden werden kann. Normalerweise lautet dieser Speicherordner „WINDOWS/inf“.*

Universal Restore-Einstellungen

Automatische Suche nach Treibern

Spezifizieren Sie, wo das Programm nach Treibern für Hardware Abstraction Layer (HAL), Festplatten-Controller und Netzwerkadapter suchen soll:

- Befinden sich die Treiber auf einer Disc (CD/DVD) des Herstellers oder einem anderen Wechselmedium, dann aktivieren Sie **Wechselmedien durchsuchen**.
- Liegen die Treiber in einem Netzwerkordner oder auf einem bootfähigen Medium, so spezifizieren Sie den Pfad zu diesem Ordner durch Anklicken von **Ordner durchsuchen**.

Während der Wiederherstellung führt Universal Restore eine rekursive Suche in allen Unterordnern des angegebenen Verzeichnisses durch, findet aus allen verfügbaren die am besten passenden HAL- und Festplatten-Controller-Treiber heraus und installiert diese in das wiederhergestellte System. Universal Restore sucht außerdem nach Treibern für Netzwerkadapter, der Pfad des gefundenen Treibers wird dann dem Betriebssystem durch Universal Restore übermittelt. Wenn die Hardware über mehrere Netzwerkkarten verfügt, so versucht Universal Restore, die Treiber aller Karten zu konfigurieren.

Auf jeden Fall zu installierende Massenspeichertreiber

Erweitern Sie zum Zugriff auf diese Einstellung den Punkt **Auf jeden Fall zu installierende Massenspeichertreiber**.

Sie benötigen diese Einstellung falls:

- Die Ziel-Hardware einen speziellen Massenspeicher-Controller wie RAID (insbesondere NVIDIA RAID) oder einen Fibre Channel-Adapter verwendet.
- Sie ein System zu einer virtuellen Maschine wiederherstellen, die einen SCSI-Festplatten-Controller verwendet und mit einem bootfähigen Medium gestartet wird. Verwenden Sie die SCSI-Treiber, die mit der Software für Ihre virtuellen Maschinen ausgeliefert werden – oder laden Sie die neueste Treiberversion von der Website des Software-Herstellers herunter.
- Die automatische Suche nach Treibern nicht hilft, das System zu booten.

Spezifizieren Sie die entsprechenden Treiber, indem Sie auf den Befehl **Treiber hinzufügen** klicken. Die hier angegebenen Treiber werden auch dann – unter entsprechenden Warnmeldungen – installiert, wenn das Programm einen besseren Treiber findet.

Der Recovery-Prozess

Falls Universal Restore an den angegebenen Speicherorten keinen kompatiblen Treiber finden kann, zeigt es zu dem Problemgerät eine Eingabeaufforderung an. Wählen Sie aus den nachfolgenden Varianten:

- Fügen Sie den Treiber einem der zuvor spezifizierten Speicherorte hinzu und klicken Sie auf **Wiederholen**.
- Wenn Sie sich nicht an den Speicherort erinnern, dann setzen Sie die Recovery-Aktion fort. Sollte das Ergebnis nicht zufriedenstellend sein, dann starten Sie Universal Restore ohne Recovery-Aktion, indem Sie in der Willkommenseite des Mediums auf den Befehl **Universal Restore anwenden** klicken. Spezifizieren Sie bei Konfiguration der Aktion den benötigten Treiber.

Sobald Windows bootet, wird es die Standardprozedur zur Installation neuer Hardware initialisieren. Der Treiber für den Netzwerkadapter wird ohne weitere Nachfrage installiert, sofern er eine Microsoft Windows-Signatur hat. Anderenfalls erfragt Windows Ihre Bestätigung zur Installation des unsignierten Treibers.

Danach können Sie die Netzwerk-Verbindung konfigurieren und Treiber für Grafikkarte, USB- und andere Geräte spezifizieren.

5.2.2.2 Universal Restore in Linux

Universal Restore kann auf Linux-Betriebssysteme mit Kernel-Version 2.6.8 oder höher angewendet werden.

Wenn Universal Restore auf ein Linux-Betriebssystem angewendet wird, dann aktualisiert es ein temporäres Dateisystem, das auch als 'Initial RAM-Disk' (initrd) bekannt ist. Dadurch wird gewährleistet, dass das Betriebssystem von neuer, abweichender Hardware booten kann.

Universal Restore fügt der 'Initial RAM-Disk' Module für die neue Hardware hinzu (inklusive Gerätetreibern). Es findet die benötigten Module üblicherweise im Verzeichnis **/lib/modules** des von Ihnen gerade wiederhergestellten Betriebssystems. Falls Universal Restore ein benötigtes Modul nicht finden kann, schreibt es den Dateinamen des Moduls in das Log (S. 372).

Universal Restore kann unter Umständen die Konfiguration des GRUB-Boot-Loaders modifizieren. Dies kann beispielsweise notwendig sein, um die Bootfähigkeit des Systems zu gewährleisten, falls die neue Maschine ein anderes Volume-Layout als die ursprüngliche hat.

Universal Restore modifiziert niemals den Linux-Kernel.

Zur ursprünglichen 'Initial RAM-Disk' zurücksetzen

Sie können bei Bedarf zur ursprünglichen 'Initial RAM-Disk' zurücksetzen.

Die 'Initial RAM-Disk' ist auf der Maschine in einer Datei gespeichert. Bevor Universal Restore die 'Initial RAM-Disk' erstmals aktualisiert, speichert es eine Kopie von dieser im gleichen Verzeichnis. Der Name der Kopie entspricht dem Namen der Datei, gefolgt von dem Suffix **_acronis_backup.img**. Diese Kopie wird auch dann nicht überschrieben, wenn Sie Universal Restore mehrmals ausführen (beispielsweise nachdem Sie fehlende Treiber hinzugefügt haben).

Nutzen Sie einen der nachfolgenden Wege, um zur ursprünglichen 'Initial RAM-Disk' zurückzusetzen:

- Benennen Sie die Kopie entsprechend um. Führen Sie beispielsweise einen Befehl ähnlich zu nachfolgendem aus:

```
mv initrd-2.6.16.60-0.21-default_acronis_backup.img
initrd-2.6.16.60-0.21-default
```

- Spezifizieren Sie die Kopie in der Zeile **initrd** der GRUB-Boot-Loader-Konfiguration (S. 177).

5.2.2.3 Universal Restore auf mehrere Betriebssysteme anwenden

Sie können Universal Restore während einer Recovery-Aktion für Betriebssysteme eines bestimmten Typs verwenden: alle Windows-Systeme, alle Linux-Systeme oder beide.

Falls Ihre Auswahl der wiederherzustellenden Volumes mehrere Windows-Systeme enthält, können Sie alle für diese gedachten Treiber in einer einzigen Liste spezifizieren. Jeder Treiber wird in das jeweilige Betriebssystem installiert, für das er vorgesehen ist.

5.3 Recovery von BIOS-basierten Systemen zu UEFI-basierten Systemen und umgekehrt

Acronis Backup & Recovery 11.5 unterstützt die Übertragung von 64-Bit-Windows-Betriebssystemen zwischen BIOS-basierter Hardware und Hardware, die 'Unified Extensible Firmware Interface' (UEFI) unterstützt.

Die Funktionsweise

Abhängig davon, ob die Maschine eine BIOS- oder UEFI-Firmware zum Booten verwendet, muss das Laufwerk mit dem System-Volumen ein bestimmtes *Partitionierungsschema* haben. Das Partitionierungsschema ist MBR (Master Boot Record) beim BIOS-Standard und GPT (GUID Partition Table) beim UEFI-Standard.

Zusätzlich reagiert auch das Betriebssystem selbst auf den Typ der Firmware.

Bei Durchführung einer Wiederherstellung auf eine Maschine, deren Firmware sich von der der ursprünglichen Maschine unterscheidet, macht Acronis Backup & Recovery 11.5 Folgendes:

- Es initialisiert das Laufwerk, zu dem Sie das System-Volume wiederherstellen, entweder als MBR- oder als GPT-Laufwerk – abhängig von der neuen Firmware.
- Es passt das Windows-Betriebssystem so an, dass es von der neuen Firmware starten kann.

Weitere Details (einschließlich einer List von Windows-Betriebssystemen, die auf diese Art angepasst werden können) finden Sie unter 'Wiederherstellung von Volumes (S. 170)' und 'Wiederherstellung von Laufwerken (S. 171)' in diesem Abschnitt.

Empfehlungen

- Stellen Sie das komplette System auf nicht initialisierte Laufwerke wieder her.
- Verwenden Sie beim Migrieren auf bzw. zu einer UEFI-basierten Hardware ein Linux-basiertes oder WinPE-basiertes (höher als Version 4.0) Boot-Medium. Ältere Versionen von WinPE und dem Acronis PXE Server unterstützen kein UEFI.
- Beachten Sie, dass der BIOS-Standard es nicht erlaubt, Laufwerksspeicherplatz mit mehr als 2 TB zu verwenden.

Beschränkungen

Die Übertragung eines Linux-Systems zwischen UEFI und BIOS wird nicht unterstützt.

Die Übertragung eines Windows-Systems zwischen UEFI und BIOS wird nicht unterstützt, falls das Backup an einem dieser Speicherorte vorliegt:

- Acronis Online Backup Storage
- Bandgerät
- Optische Datenträger (CDs, DVDs oder Blu-ray-Medien)

Sollte die Übertragung eines Systems zwischen UEFI und BIOS nicht unterstützt werden, dann initialisiert Acronis Backup & Recovery 11.5 das Ziellaufwerk mit demselben Partitionierungsschema wie das ursprüngliche Laufwerk. Dabei erfolgt keine Anpassung des Betriebssystems. Sollte die Zielmaschine sowohl UEFI wie auch BIOS unterstützen, dann müssen Sie noch den zur ursprünglichen Maschine passenden Boot-Mode aktivieren. Anderenfalls wird das System nicht mehr booten.

5.3.1 Volumes wiederherstellen

Angenommen, Sie haben ein Backup der System- und Boot-Volumes durchgeführt (oder der kompletten Maschine) und wollen diese Volumes nun zu einer anderen Plattform wiederherstellen. Die Fähigkeit des wiederhergestellten Systems zu booten, hängt von folgenden Faktoren ab:

- **Betriebssystem der Quelle:** ist das Betriebssystem konvertierbar oder nicht? Konvertierbare Betriebssystem erlauben es, den Boot-Modus von BIOS zu UEFI zu konvertieren (und zurück).
  - Die 64-Bit-Versionen aller Windows-Betriebssysteme (beginnend mit Windows Vista x64 SP1) sind konvertierbar.
  - Die 64-Bit-Versionen aller Windows Server-Betriebssysteme (beginnend mit Windows Server 2008 x64 SP1) sind konvertierbar.

  Alle anderen Betriebssysteme sind nicht konvertierbar.
- **Partitionsschema von Quell- und Ziellaufwerk**: MBR oder GPT. Die System- und Boot-Volumes von BIOS-Plattformen verwenden MBR-Laufwerke. Die System- und Boot-Volumes von UEFI-Plattformen verwenden GPT-Laufwerke.

  Wenn Sie bei einer Wiederherstellung ein nicht initialisiertes Ziellaufwerks auswählen, wird das Laufwerk automatisch zu GPT oder MBR initialisiert – in Abhängigkeit vom Partitionsschema des ursprünglichen Laufwerks, dem aktuellen Boot-Modus (UEFI oder BIOS) und dem Typ der auf diesem Volume vorhandenen Betriebssysteme (konvertierbar oder 'nicht konvertierbar').

  Falls die Initialisierung zum Verlust der Bootfähigkeit führen kann, verwendet die Software – unter Ignorieren der Größe des Ziellaufwerks – das Partitionsschema des Quell-Volumes. In solchen Fällen kann die Software für Laufwerke, die größer als 2 TB sind, das MBR-Partitionierungsschema wählen – wobei der Speicherplatz oberhalb von 2 TB jedoch nicht nutzbar ist.

  Sie können das Ziellaufwerk bei Bedarf auch manuell initialisieren, indem Sie die Funktion zur Laufwerksverwaltung (S. 300) verwenden.

Die folgenden Tabelle fasst zusammen, ob die Bootfähigkeit eines Systems erhalten werden kann, wenn Sie Boot- und System-Volumes eines BIOS-basierten auf ein UEFI-basiertes System wiederherstellen (und umgekehrt).

- Ein grüner Hintergrund bedeutet, dass das System boofähig sein wird. Es ist kein Benutzereingriff erforderlich.
- Ein gelber Hintergrund bedeutet, dass Sie zusätzliche Schritte durchführen müssen, um das System bootfähig zu machen. Diese Schritte sind auf einigen Maschinen jedoch nicht möglich.
- Ein roter Hintergrund bedeutet, dass das System aufgrund von Beschränkungen der BIOS- bzw. UEFI-Plattform nicht bootfähig sein wird.

<table>
<tr><th rowspan="2">Ursprüngliches System</th><th colspan="4">Ziel-Hardware</th></tr>
<tr><td>BIOS
Laufwerk: MBR</td><td>BIOS
Laufwerk: GPT</td><td>UEFI
Laufwerk: MBR</td><td>UEFI
Laufwerk: GPT</td></tr>
<tr><td>BIOS
Betriebssystem: konvertierbar</td><td rowspan="2"></td><td rowspan="2">Lösung
Stellen Sie das Betriebssystem zu einem MBR-Laufwerk oder einem nicht initialisierten Laufwerk wieder her.</td><td rowspan="2">Die Zielmaschine muss BIOS unterstützen.
Zusätzliche Schritte
1. Schalten Sie vor der Wiederherstellung den UEFI-Modus im BIOS aus
2. Führen Sie die Wiederherstellung mit einem bootfähigen Medium aus.
oder
Schalten Sie nach der Wiederherstellung den UEFI-Modus im BIOS aus.</td><td>Ein konvertierbares Betriebssystem wird automatisch zur Unterstützung von UEFI zum Booten konvertiert.</td></tr>
<tr><td>BIOS
Betriebssystem: nicht konvertierbar</td><td>Lösung
Stellen Sie das Betriebssystem zu einem MBR-Laufwerk oder einem nicht initialisierten Laufwerk wieder her.</td></tr>
<tr><td>UEFI
Betriebssystem: konvertierbar</td><td>Ein konvertierbares Betriebssystem wird automatisch zur Unterstützung des BIOS-Modus zum Booten konvertiert.</td><td rowspan="2">Die Zielmaschine muss UEFI unterstützen.
Zusätzliche Schritte
1. Schalten Sie vor der Wiederherstellung den UEFI-Modus im BIOS an.
2. Führen Sie die Wiederherstellung mit einem bootfähigen Medium aus.
oder
Schalten Sie nach der Wiederherstellung den UEFI-Modus im BIOS an.</td><td rowspan="2">Lösung
Stellen Sie das Betriebssystem zu einem GPT-Laufwerk oder einem nicht initialisierten Laufwerk wieder her.</td><td rowspan="2"></td></tr>
<tr><td>UEFI
Betriebssystem: nicht konvertierbar</td><td>Lösung
Stellen Sie das Betriebssystem zu einem GPT-Laufwerk oder einem nicht initialisierten Laufwerk wieder her.</td></tr>
</table>

5.3.2 Laufwerke wiederherstellen

Angenommen, Sie haben ein komplettes Laufwerk (mit all seinen Volumes) per Backup gesichert und wollen nun dieses Laufwerk zu einer anderen Zielplattform wiederherstellen.

Die Fähigkeit des wiederhergestellten Systems, in verschiedenen Modi booten zu können, hängt von den auf dem Quelllaufwerk installierten Betriebssystemen ab. Betriebssysteme können **konvertierbar** sein, d.h. einen Wechsel des Boot-Modus von BIOS zu UEFI (und zurück) erlauben –

oder eben **nicht konvertierbar** sein. Eine Liste konvertierbarer Betriebssysteme finden Sie unter 'Volumes wiederherstellen (S. 170)'.

- Wenn ein Quelllaufwerk ein oder mehrere Betriebssysteme enthält und *alle* davon konvertierbar sind, dann kann der Boot-Modus automatisch gewechselt werden. In Abhängigkeit vom aktuellen Boot-Modus wird das Ziellaufwerk möglicherweise entweder mit dem GPT- oder MBR-Partitionsschema initialisiert.
- Falls *mindestens ein* Betriebssystem auf dem Quelllaufwerk 'nicht konvertierbar' ist (oder das Quelllaufwerk ein Boot-Volume eines 'nicht konvertierbaren' Betriebssystems enthält), dann kann der Boot-Modus nicht automatisch gewechselt werden und wird die Software das Ziellaufwerk wie das Quelllaufwerk initialisieren. Um die Zielmaschine booten zu können, müssen Sie den UEFI-Modus im BIOS manuell ein- bzw. ausschalten. Anderenfalls wird das System nach der Wiederherstellung nicht mehr booten.

Die folgende Tabelle fasst alle Wiederherstellungsvarianten von Laufwerken eines BIOS-basierten zu einem UEFI-basierten System (und umgekehrt) zusammen.

- Ein grüner Hintergrund bedeutet, dass das System boofähig sein wird. Es ist kein Benutzereingriff erforderlich.
- Ein gelber Hintergrund bedeutet, dass Sie zusätzliche Schritte durchführen müssen, um das System bootfähig zu machen. Diese Schritte sind auf einigen Maschinen jedoch nicht möglich.

Ursprüngliches System	**Ziel-Hardware**	
	BIOS	UEFI
BIOS Betriebssystem: konvertierbar		Das Ziellaufwerk wird als GPT initialisiert. Das Betriebssystem wird automatisch zur Unterstützung von UEFI zum Booten konvertiert. Falls Sie das Quelllaufwerk 'wie vorliegend' wiederherstellen wollen: 1. Schalten Sie den UEFI-Modus im BIOS aus. 2. Starten Sie mit einem bootfähigen Medium und führen Sie die Wiederherstellung aus.
BIOS Betriebssystem: nicht konvertierbar		Das Ziellaufwerk wird wie das Quelllaufwerk initialisiert (MBR). *Die Zielmaschine muss BIOS unterstützen.* **Zusätzliche Schritte** 1. Schalten Sie den UEFI-Modus im BIOS aus. 2. Starten Sie mit einem bootfähigen Medium und führen Sie die Wiederherstellung aus.

Ursprüngliches System	Ziel-Hardware	
	BIOS	UEFI
UEFI Betriebssystem: konvertierbar	Das Ziellaufwerk wird als MBR initialisiert. Das Betriebssystem wird automatisch konvertiert, um das Booten per BIOS zu unterstützen. Falls Sie das Quelllaufwerk 'wie vorliegend' wiederherstellen wollen: 1. Schalten Sie den UEFI-Modus im BIOS ein. 2. Starten Sie mit einem bootfähigen Medium und führen Sie die Wiederherstellung aus.	
UEFI Betriebssystem: nicht konvertierbar	Das Ziellaufwerk wird wie das Quelllaufwerk initialisiert (GPT). *Die Zielmaschine muss UEFI unterstützen.* **Zusätzliche Schritte** 1. Schalten Sie den UEFI-Modus im BIOS ein. 2. Starten Sie mit einem bootfähigen Medium und führen Sie die Wiederherstellung aus.	

Wiederherstellung auf große Laufwerk in einem BIOS-System

Nach einer Wiederherstellung zu einem BIOS-basierten System wird das Zielsystemlaufwerk als MBR initialisiert. Aufgrund der Laufwerksgrößenbeschränkung im BIOS-Standard stehen für Laufwerke, die größer sind als 2 TB, nur die ersten 2 TB des Laufwerkspeicherplatzes zur Verfügung. Sollte die Maschine UEFI unterstützen, dann lässt sich diese Beschränkung umgehen, indem Sie den UEFI-Modus einschalten und dann die Wiederherstellung durchführen. Das Laufwerk wird nach dem GPT-Standard initialisiert. Bei GPT-Laufwerken existiert keine 2 TB-Beschränkung.

5.4 Acronis Active Restore

Active Restore ist eine geschützte Acronis-Technologie, die ein System oder eine Datenbank direkt verfügbar macht, sobald die Wiederherstellung gestartet wurde.

Dieser Abschnitt beschreibt die Verwendung von Active Restore bei Wiederherstellung eines Betriebssystems. Obwohl auf der gleichen Technologie basierend, verlaufen Wiederherstellungen von Microsoft Exchange- oder Microsoft SQL-Datenbanken auf unterschiedliche Art. Siehe folgende Abschnitte für weitere Informationen:

- Zur Wiederherstellung von Microsoft Exchange-Datenbanken siehe den Abschnitt 'Der Einsatz von Acronis Active Restore zur Datenbankwiederherstellung' im Dokument 'Backups von Microsoft Exchange-Server-Daten'.
- Zur Wiederherstellung von Microsoft SQL-Datenbanken siehe den Abschnitt 'Der Einsatz von Acronis Active Restore zur SQL-Datenbankwiederherstellung (S. 352)'.

Beschränkungen

- Active Restore ist nicht verfügbar, wenn Sie Windows 8/8.1 oder Windows Server 2012/2012 R2 wiederherstellen.
- Active Restore ist zur sofortigen Datenwiederherstellung auf der gleichen Maschine gedacht. Bei Wiederherstellungen auf abweichende Hardware steht es nicht zur Verfügung.
- Der einzig unterstützte Archiv-Speicherort ist ein lokales Laufwerk oder, um präziser zu sein, jedes über das BIOS der Maschine ansprechbare Gerät. Das kann die Acronis Secure Zone, eine USB-Festplatte, ein USB-Stick oder jede interne Festplatte sein.
- Active Restore unterstützt keine Laufwerke mit GPT-Partitionierungsschema bei Wiederherstellungsaktionen (weder als Quelle noch als Ziel) und auch nicht als Archiv-Speicherort. Das bedeutet auch, dass UEFI (Unified Extensible Firmware Interface) nicht unterstützt wird. Der einzige unterstützte Boot-Modus ist BIOS.

Die Funktionsweise

Beim Konfigurieren einer Wiederherstellungsaktion wählen Sie die Laufwerke bzw. Volumes, um diese aus einem Backup wiederherzustellen. Acronis Backup & Recovery 11.5 scannt die gewählten, im Backup befindlichen Festplatten oder Laufwerke. Findet der Scan dabei ein unterstütztes Betriebssystem, so wird Acronis Active Restore verfügbar.

Sofern Sie Active Restore nicht aktivieren, erfolgt die Systemwiederherstellung auf die übliche Art und wird die Maschine erst nach vollständiger Wiederherstellung wieder einsatzbereit.

Falls Sie Active Restore aktivieren, wird die Sequenz der Aktionen folgendermaßen festgelegt:

Sobald die Systemwiederherstellung gestartet ist, bootet das Betriebssystem aus dem Backup heraus. Die Maschine wird einsatzfähig und steht bereit, um notwendige Dienste anzubieten. Die für eingehende Anforderungen notwendigen Daten werden mit der höchsten Priorität, alle anderen im Hintergrund wiederhergestellt.

Da die Bedienung solcher Anforderungen simultan zur Wiederherstellung erfolgt, kann das Betriebssystem ausgebremst werden – auch dann, wenn in den Recovery-Optionen die Recovery-Priorität (S. 189) auf **Niedrig** eingestellt wurde. Obwohl die Systemausfallzeit minimal ist, kann es während der Wiederherstellung zu einer verringerten Performance kommen.

Einsatzszenarien

1. Die Verfügbarkeit eines Systems gehört zu den Effizienzkriterien.

   Beispiele: Client-bezogene Online-Dienste, Web-Einzelhändler, Wahllokale

2. Das Verhältnis von System zu Speicherplatz ist stark in Richtung Speicher verzerrt.

   Einige Maschinen werden als Speicheranlagen genutzt, wobei das Betriebssystem nur ein kleines Speichersegment beansprucht, während der restliche Festplattenplatz der Archivierung dient, etwa für Videos, Audio- oder andere Multimedia-Dateien. Einige dieser Speicher-Laufwerke können verglichen zum System extrem groß sein, so dass praktisch die komplette Wiederherstellungszeit der Rückgewinnung der Dateien gewidmet wird, obwohl sie erst später gebraucht werden könnten (wenn in naher Zukunft überhaupt).

   Entscheiden Sie sich dagegen für Acronis Active Restore, so wird das System in kurzer Zeit wieder einsatzfähig sein. Benutzer werden in die Lage versetzt, benötigte Dateien aus dem Datenspeicher zu öffnen und zu verwenden, während alle restlichen, nicht sofort benötigten Dateien im Hintergrund weiter wiederhergestellt werden.

   Beispiele: Datenspeicher für Film- oder Musiksammlungen bzw. Multimedia-Dateien

Anwendung

1. Speichern Sie das Backup des Systemlaufwerks bzw. -volumes an einer Position, auf die über das System-BIOS zugegriffen werden kann. Das kann die Acronis Secure Zone, eine USB-Festplatte, ein USB-Stick oder jede interne Festplatte sein.

   Falls Betriebssystem und Boot-Loader auf unterschiedlichen Volumes liegen, nehmen Sie immer beide mit in das Backup auf. Diese Laufwerke müssen auch zusammen wiederhergestellt werden, da anderenfalls ein hohes Risiko besteht, dass das Betriebssystem nicht mehr startet.

2. Erstellen Sie ein bootfähiges Medium.
3. Booten Sie die Maschine mit einem bootfähigen Medium, wenn es zu einem Systemausfall kommt. Starten Sie die Konsole und verbinden Sie sich mit dem bootfähigen Agenten.
4. Erstellen Sie einen Recovery-Task (S. 146). Stellen Sie bei **Recovery-Quelle** sicher, dass das System-Laufwerk oder System-Volume für die Wiederherstellung ausgewählt wurde.

   Acronis Active Restore wählt für das Hochfahren und die nachfolgende Wiederherstellung das erste beim Backup-Scan gefundene Betriebssystem. Versuchen Sie nicht, mehr als ein Betriebssystem unter Verwendung von Active Restore wiederherzustellen, damit die Ergebnisse berechenbar bleiben. Wählen Sie auch bei Wiederherstellung eines Multi-Boot-Systems nur jeweils ein System-Volume und Boot-Volume.

5. Stellen Sie bei **Recovery-Ziel** sicher, dass das System-Laufwerk oder System-Volume dem ersten Laufwerk zugeordnet ist. Sollte dem nicht so sein, dann führen Sie eine manuelle Zuordnung durch (wie im Abschnitt 'Ziellaufwerke wählen (S. 154)' beschrieben).
6. Wählen Sie bei **Acronis Active Restore** die Option **Verwenden**.
7. Sobald die Systemwiederherstellung gestartet ist, bootet das Betriebssystem aus dem Backup heraus. Das Acronis Active Restore-Symbol erscheint im Infobereich der Taskleiste. Die Maschine wird einsatzfähig und steht bereit, um notwendige Dienste anzubieten. Ein das System sofort benutzender Anwender sieht den Verzeichnisbaum mit seinen Symbolen, kann Dateien öffnen oder Anwendungen starten, selbst wenn diese noch nicht wiederhergestellt wurden.

   Die Treiber von Acronis Active Restore fangen Systemanfragen ab und setzen Dateien, die zur Erfüllung einkommender Anfragen notwendig sind, auf höchste Wiederherstellungspriorität. Und während diese 'on-the-fly'-Wiederherstellung fortschreitet, wird der noch andauernde Wiederherstellungsprozess in den Hintergrund transferiert.

   Solange die Recovery-Aktion nicht abgeschlossen ist, sollten Sie nicht versuchen, die Maschine herunterzufahren oder einen Neustart durchzuführen. Falls Sie Ihr Maschine ausschalten, gehen alle seit dem letzten Systemstart durchgeführten Änderungen verloren. Das System wird dann nicht wiederhergestellt, auch nicht partiell. Die einzig verbliebene Lösung in diesem Fall ist es dann, den Wiederherstellungsprozess von einem bootfähigen Medium aus neu zu starten.

8. Die Hintergrund-Wiederherstellung geht solange weiter, bis alle gewählten Laufwerke wiederhergestellt wurden, alle Ereignismeldungen gemacht wurden und das Acronis Active Restore-Symbol aus dem Infobereich der Taskleiste verschwindet.

5.5 Troubleshooting zur Bootfähigkeit

Wenn ein System zum Zeitpunkt seines Backups bootfähig war, erwarten Sie auch, dass es nach einer Wiederherstellung booten kann. Informationen, die das Betriebssystem zum Booten speichert und verwendet, können jedoch bei einer Wiederherstellung ungültig werden, insbesondere, wenn Sie die Volume-Größe, die Speicherorte oder die Ziellaufwerke ändern. Acronis Backup & Recovery 11.5 aktualisiert Windows Boot-Loader automatisch nach einer Wiederherstellung. Auch andere Boot-Loader werden möglicherweise repariert, es gibt jedoch Fälle, bei denen Sie selbst die Loader reaktivieren müssen. Speziell, wenn Sie Linux-Volumes wiederherstellen, ist es manchmal notwendig,

Fehlerkorrekturen anzuwenden oder Boot-Veränderungen durchzuführen, damit Linux korrekt startet und geladen werden kann.

Nachfolgend eine Zusammenfassung typischer Situationen, die zusätzliche Benutzereingriffe benötigen.

Warum ein wiederhergestelltes Betriebssystem nicht mehr bootfähig sein kann

- **Das BIOS der Maschine ist so konfiguriert, dass es von einem anderen Laufwerk bootet.**

  Lösung: Konfigurieren Sie das BIOS so, dass es von dem Laufwerk bootet, auf dem das Betriebssystem liegt.

- **Das System wurde auf abweichender Hardware wiederhergestellt und die neue Hardware ist inkompatibel mit den wichtigsten im Backup enthaltenen Treibern,**

  Lösung: Starten Sie die Maschine mit einem bootfähigen Medium und wenden Sie Acronis Universal Restore an (S. 165), um die passenden Treiber und Module zu installieren.

- **Windows wurde zu einem dynamischen Volume wiederhergestellt, das nicht bootfähig sein kann.**

  Lösung: Führen Sie eine Wiederherstellung von Windows auf ein Volume vom Typ 'Basis', 'Einfach' oder 'Gespiegelt' durch.

- **Ein System-Volume wurde zu einem Laufwerk wiederhergestellt, das keinen MBR hat.**

  Wenn Sie die Wiederherstellung eines System-Volumes auf einem Laufwerk ohne MBR konfigurieren, fragt Sie das Programm, ob Sie zusammen mit dem System-Volume auch den MBR wiederherstellen wollen. Entscheiden Sie sich nur dann gegen eine Wiederherstellung, wenn Sie nicht wollen, dass das System bootfähig wird.

  Lösung: Stellen Sie das Volume zusammen mit dem MBR dem korrespondierenden Laufwerk wieder her.

- **Das System verwendet den Acronis OS Selector**

  Weil der Master Boot Record (MBR) während der System-Wiederherstellung ausgetauscht werden kann, ist es möglich, dass der Acronis OS Selector, der den MBR verwendet, funktionsunfähig wird. Reaktivieren Sie den Acronis OS Selector folgendermaßen, wenn dies passieren sollte:

  Lösung: Starten Sie die Maschine mit dem bootfähigen Medium des Acronis Disk Director und wählen Sie im Menü **Extras –> OS Selector aktivieren**.

- **Das System verwendet den GRand Unified Bootloader (GRUB) und wurde von einem normalen Backup (nicht 'Raw' bzw. Sektor-für-Sektor) wiederhergestellt.**

  Ein Teil des GRUB-Loaders liegt entweder in den ersten Sektoren des Laufwerks oder in den ersten Sektoren des Volumes. Der Rest befindet sich im Dateisystem einer der Volumes. Die Bootfähigkeit des Systems kann nur dann automatisch wiederhergestellt werden, wenn GRUB innerhalb der ersten Sektoren des Laufwerks sowie im Dateisystem liegt, zu dem ein direkter Zugriff möglich ist. In allen anderen Fällen muss der Benutzer den Boot-Loader manuell reaktivieren.

  Lösung: Reaktivieren Sie den Boot-Loader. Sie müssen möglicherweise auch noch die Konfigurationsdatei reparieren.

- **Das System verwendet Linux Loader (LILO) und wurde von einem normalen Backup (nicht 'Raw' bzw. Sektor-für-Sektor) wiederhergestellt.**

  LILO enthält zahlreiche Verweise zu absoluten Sektor-Nummern und kann daher nicht automatisch repariert werden, außer wenn alle Daten genau zu denjenigen Sektoren wiederhergestellt werden, die dieselben absoluten Nummern wie auf dem Quelllaufwerk haben.

Lösung: Reaktivieren Sie den Boot-Loader. Sie müssen außerdem möglicherweise aus dem im vorherigen Punkt genannten Grund die Konfigurationsdatei des Loaders reparieren.

- **Der System-Loader verweist auf das falsche Volume**

  Dies kann passieren, wenn System- bzw. Boot-Volumes nicht zu ihrer ursprünglichen Position wiederhergestellt werden.

  Lösung: Für Windows-Loader wird dies durch eine Anpassung der Dateien 'boot.ini' bzw. 'boot/bcd' behoben. Acronis Backup & Recovery 11.5 führt dies automatisch durch und daher ist es unwahrscheinlich, dass Sie dieses Problem erleben.

  Für die Loader von GRUB und LILO müssen Sie die Konfigurationsdateien korrigieren. Hat sich die Nummer der Linux Root-Partition verändert, so ist es außerdem empfehlenswert, dass Sie '/etc/fstab' anpassen, damit korrekt auf das SWAP-Laufwerk zugegriffen werden kann.

- **Linux wurde von einem LVM-Volume-Backup auf ein Basis-MBR-Laufwerk wiederhergestellt.**

  Ein solches System kann nicht booten, weil sein Kernel versucht, das Root-Dateisystem von der LVM-Volume zu mounten.

  Lösung: Ändern Sie die Konfiguration des Loaders und '/etc/fstab' – so dass LVM nicht mehr verwendet wird – und reaktivieren Sie den Boot-Loader.

5.5.1 So reaktivieren Sie GRUB und ändern die Konfiguration

Für gewöhnlich sollten Sie die passende Prozedur in den Unterlagen zum Boot-Loader nachschlagen. Es gibt auch den entsprechenden Artikel in der Knowledge Base auf der Acronis-Website.

Nachfolgend ein Beispiel, wie Sie GRUB reaktivieren, wenn das Systemlaufwerk (Volume) auf identische Hardware wiederhergestellt wird.

1. Starten Sie Linux oder starten Sie von einem bootfähigen Medium und drücken Sie dann Strg+Alt+F2.
2. Mounten Sie das System, das Sie wiederherstellen:

```
mkdir /mnt/system/
mount -t ext3 /dev/sda2 /mnt/system/ # root partition
mount -t ext3 /dev/sda1 /mnt/system/boot/ # boot partition
```

3. Mounten Sie die Dateisysteme **proc** und **dev** an das wiederherzustellende System:

```
mount -t proc none /mnt/system/proc/
mount -o bind /dev/ /mnt/system/dev/
```

4. Sichern Sie eine Kopie der „menu“-Datei von GRUB, indem Sie einen der folgenden Befehle ausführen:

```
cp /mnt/system/boot/grub/menu.lst /mnt/system/boot/grub/menu.lst.backup
```

   oder

```
cp /mnt/system/boot/grub/grub.conf /mnt/system/boot/grub/grub.conf.backup
```

5. Bearbeiten Sie die Datei **/mnt/system/boot/grub/menu.lst** (für Debian-, Ubuntu- und SUSE Linux-Distributionen) oder die Datei **/mnt/system/boot/grub/grub.conf** (für Fedora- und Red Hat Enterprise Linux-Distributionen) — z.B. wie folgt:

```
vi /mnt/system/boot/grub/menu.lst
```

6. Suchen Sie in der Datei **menu.lst** (alternativ **grub.conf**) den Menü-Eintrag, der zu dem von Ihnen wiederhergestellten System korrespondiert. Dieser Menü-Eintrag sieht folgendermaßen aus:

```
title Red Hat Enterprise Linux Server (2.6.24.4)
      root (hd0,0)
      kernel /vmlinuz-2.6.24.4 ro root=/dev/sda2 rhgb quiet
      initrd /initrd-2.6.24.4.img
```


Die Zeilen, die mit **title**, **root**, **kernel** bzw. **initrd** beginnen, legen Folgendes fest:

- Den Titel des Menü-Eintrages.
- Das Gerät, auf dem sich der Linux-Kernel befindet – üblicherweise die Boot- oder root-Partition, im vorliegenden Beispiel **root (hd0,0)**.
- Der Pfad zum Kernel auf diesem Gerät und der root-Partition – im vorliegenden Beispiel ist der Pfad **/vmlinuz-2.6.24.4** und die root-Partition ist **/dev/sda2**. Sie können die root-Partition über ihre Bezeichnung (in der Form von **root=LABEL=/**), den Identifier (in der Form von **root=UUID=***some_uuid*) oder den Gerätenamen (**root=/dev/sda2**) spezifizieren.
- Der Pfad zum Dienst **initrd** auf diesem Gerät.

7. Bearbeiten Sie die Datei **/mnt/system/etc/fstab**, um die Namen all der Geräte zu korrigieren, die sich als Ergebnis der Wiederherstellung verändert haben.
8. Starten Sie die Shell von GRUB, indem Sie einen der folgenden Befehle ausführen:

   ```
   chroot /mnt/system/ /sbin/grub
   ```

   oder

   ```
   chroot /mnt/system/ /usr/sbin/grub
   ```

9. Spezifizieren Sie das Laufwerk, auf dem sich GRUB befindet – üblicherweise die Boot- oder root-Partition.

   ```
   root (hd0,0)
   ```

10. Installieren Sie GRUB. Um GRUB z.B. in den Master Boot Record (MBR) der ersten Festplatte zu installieren, führen Sie den folgenden Befehl aus:

    ```
    setup (hd0)
    ```

11. Benden Sie die Shell von GRUB:

    ```
    quit
    ```

12. Trennen Sie die gemounteten Datei-Systeme und starten Sie dann neu:

    ```
    umount /mnt/system/dev/
    umount /mnt/system/proc/
    umount /mnt/system/boot/
    umount /mnt/system/
    reboot
    ```

13. Rekonfigurieren Sie den Boot-Loader durch die Verwendung von Tools und der Dokumentation, die zur von Ihnen verwendeten Linux-Distribution gehört. In Debian und Ubuntu z.B. müssen Sie vermutlich einige kommentierte Zeilen in der Datei **/boot/grub/menu.lst** bearbeiten und dann das Script **update-grub** ausführen; ansonsten treten die Änderungen nicht in Kraft.

5.5.2 Über Windows-Loader

Windows NT/2000/XP/2003

Ein Teil der Loader ist im Boot-Sektor hinterlegt, der Rest befindet sich in den Dateien ntldr, boot.ini, ntdetect.com, ntbootdd.sys. Boot.ini ist eine Textdatei, die die Konfiguration des Loaders enthält. Beispiel:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional"
/noexecute=optin /fastdetect
```

Windows Vista und später

Ein Teil des Loaders ist im Boot-Sektor hinterlegt, der Rest in den Dateien bootmgr und boot\bcd. Während des Windows-Starts wird boot\bcd in den Registry-Schlüssel HKLM \BCD00000000 gemountet.

5.6 Ein Windows-System auf Werkseinstellungen zurücksetzen

Falls Ihr Windows-Betriebssystem unter Verwendung von Acronis Backup & Recovery 11.5 für System Builders bereitgestellt wurde, dann können Sie das System auf seine Werkseinstellungen zurücksetzen.

Das Zurücksetzen des Systems auf seine Werkseinstellungen kann von der Management Konsole oder beim Booten gestartet werden. Die zweite Methode ist nützlich, wenn das Betriebssystem aus irgendeinem Grund seine Bootfähigkeit verloren hat.

- Klicken Sie, um die Aktion von der Management Konsole aus zu starten, auf den Befehl **Auf Werkseinstellungen zurücksetzen** (in der **Willkommensseite**).
- Drücken Sie, um die Aktion beim Booten zu starten, einen 'Hot Key' (üblicherweise F11) und klicken Sie in der erscheinenden Anzeige dann auf **Auf Werkseinstellungen zurücksetzen**. Alternativ können Sie auch mit dem Booten des Betriebssystems fortfahren.

Sobald Sie die Aktion bestätigen, wird Acronis Backup & Recovery 11.5 das Image der Werkskonfiguration (Factory Image), welches in der Acronis Secure Zone gespeichert ist, erneut bereitstellen. Dadurch werden das ursprüngliche Volume-Layout, das vorinstallierte Windows-Betriebssystem und mögliche ursprüngliche Dritthersteller-Anwendungen wiederhergestellt, Die Software entfernt zusätzlich alle Benutzer-Archive aus der Acronis Secure Zone und setzt die Acronis Secure Zone wieder auf ihre ursprüngliche Größe zurück.

Vorsicht: *Alle auf den ursprünglichen Laufwerken der Maschine gespeicherten Benutzerdaten gehen verloren.*

Manchmal kann ein System nicht auf die Werkseinstellungen zurückgesetzt werden, auch nicht beim Booten. Das kann beispielsweise der Fall sein, wenn es zu einem Laufwerksfehler kommt, falls das Factory Image in der Acronis Secure Zone beschädigt wurde oder das ursprüngliche Laufwerk durch ein neues ersetzt wurde. In diesem Fall können Sie das System dennoch auf die Werkseinstellungen zurücksetzen – und zwar, indem Sie das 'Bootfähige Medium mit Werkseinstellungen' (Factory Bootable Media) verwenden, sofern es mit Ihrer Maschine ausgeliefert wurde.

Booten Sie, um die Aktion zu starten, die Maschine mit diesem 'Factory Bootable Media' und klicken Sie in der erscheinenden Anzeige auf **Auf Werkseinstellungen zurücksetzen**. Sobald Sie die Aktion bestätigen, wird Acronis Backup & Recovery 11.5 eine Acronis Secure Zone erstellen und das Factory Image dorthin kopieren. Danach wird es das Factory Image, so wie weiter oben beschrieben, erneut bereitstellen.

Weitere Informationen finden Sie unter 'Acronis Secure Zone (S. 217)' und 'Acronis Startup Recovery Manager (S. 297)'.

5.7 Standardoptionen für Recovery

Jeder Acronis Agent hat eigene Standardoptionen für Recovery. Sobald ein Agent installiert ist, haben die Standardoptionen vordefinierte Werte, die in der Dokumentation als **Voreinstellungen** bezeichnet werden. Bei Erstellung eines Recovery-Tasks können Sie entweder eine Standardoption

verwenden oder diese mit einem benutzerdefinierten Wert überschreiben, der nur für diesen Task gültig ist.

Sie können außerdem auch eine Standardoption konfigurieren, indem Sie den vordefinierten Wert verändern. Der neue Wert wird dann als Standard für alle nachfolgend auf dieser Maschine erstellten Recovery-Tasks verwendet.

Um die Standardoptionen für Recovery einsehen und verändern zu können, verbinden Sie die Konsole mit der verwalteten Maschine und wählen Sie dort aus dem Hauptmenü die Befehle **Optionen –> Standardoptionen für Backup und Recovery –> Standardoptionen für Recovery**.

Verfügbarkeit der Recovery-Optionen

Art und Umfang der verfügbaren Recovery-Optionen sind abhängig von:

- Der Umgebung, in welcher der Agent arbeitet (Windows, Linux, bootfähiges Medium)
- Dem Datentyp, der gesichert wird (Laufwerke, Dateien).
- Dem Betriebssystem, das aus dem Laufwerk-Backup wiederhergestellt wird (Windows, Linux).

Die nachfolgende Tabelle fasst die Verfügbarkeit der Recovery-Optionen zusammen:

	Agent für Windows		**Agent für Linux**		**Bootfähiges Medium (Linux-basiert oder PE-basiert)**	
	Laufwerk-Recovery	**Datei-Recovery (auch aus Laufwerk-Backup)**	**Laufwerk-Recovery**	**Datei-Recovery (auch aus Laufwerk-Backup)**	**Laufwerk-Recovery**	**Datei-Recovery (auch aus Laufwerk-Backup)**
Erweiterte Einstellungen (S. 181):						
Backup-Archiv vor Wiederherstellung prüfen	+	+	+	+	+	+
Maschine automatisch neu starten, wenn dies zur Wiederherstellung erforderlich ist	+	+	+	+	-	-
Nach Abschluss der Wiederherstellung die Maschine automatisch neu starten	-	-	-	-	+	+
Dateisystem nach Wiederherstellung prüfen	+	-	+	-	+	-
SID nach Wiederherstellung ändern	Windows-Recovery	-	Windows-Recovery	-	Windows-Recovery	-
Aktuelles Datum und Zeit für wiederhergestellte Dateien festlegen	-	+	-	+	-	+

	Agent für Windows		Agent für Linux		Bootfähiges Medium (Linux-basiert oder PE-basiert)	
	Laufwerk-Recovery	Datei-Recovery (auch aus Laufwerk-Backup)	Laufwerk-Recovery	Datei-Recovery (auch aus Laufwerk-Backup)	Laufwerk-Recovery	Datei-Recovery (auch aus Laufwerk-Backup)
Fehlerbehandlung (S. 182):						
Während der Durchführung keine Meldungen bzw. Dialoge zeigen (Stiller Modus)	+	+	+	+	+	+
Bei Fehler erneut versuchen	+	+	+	+	+	+
Ereignisverfolgung:						
Ereignisanzeige von Windows (S. 184)	+	+	-	-	-	-
SNMP (S. 183)	+	+	+	+	-	-
Sicherheit auf Dateiebene (S. 184):						
Dateien mit ihren Sicherheitseinstellungen wiederherstellen	-	+	-	+	-	+
Mount-Punkte (S. 185)	-	+	-	-	-	-
Benachrichtigungen:						
E-Mail (S. 185)	+	+	+	+	-	-
Win Pop-up (S. 186)	+	+	+	+	-	-
Vor-/Nach-Befehle für Wiederherstellung (S. 187)	+	+	+	+	nur PE	nur PE
Recovery-Priorität (S. 189)	+	+	+	+	-	-

5.7.1 Erweiterte Einstellungen

Spezifizieren Sie die zusätzlichen Einstellungen für das Recovery durch Aktivieren oder Deaktivieren der folgenden Kontrollkästchen.

Aktuelles Datum und Zeit für wiederhergestellte Dateien festlegen

Diese Option ist nur wirksam, wenn Dateien wiederhergestellt werden.

Voreinstellung ist: **Aktiviert**.

Diese Option definiert, ob der Zeitstempel der wiederhergestellten Dateien aus dem Archiv übernommen wird oder ob den Dateien das aktuelle Datum und die aktuelle Zeit zugewiesen werden.

Backups vor Wiederherstellung validieren

Voreinstellung ist: **Deaktiviert**.

Diese Option definiert, ob ein Backup vor der Wiederherstellung der darin enthaltenen Daten zu validieren ist, um sicherzustellen, dass das Backup nicht beschädigt ist.

Dateisystem nach Wiederherstellung prüfen

Diese Option ist nur wirksam, wenn Laufwerke oder Volumes wiederhergestellt werden.

Voreinstellung ist: **Deaktiviert**.

Diese Option definiert, ob nach der Wiederherstellung eines Laufwerks oder Volumes die Integrität des wiederhergestellten Dateisystems geprüft wird. Die Überprüfung wird entweder direkt nach der Wiederherstellung ausgeführt oder nachdem die Maschine mit dem wiederhergestellten Betriebssystem gebootet hat.

Maschine automatisch neu starten, wenn dies zur Wiederherstellung erforderlich ist

Diese Option ist wirksam, wenn die Wiederherstellung auf einer Maschine mit laufendem Betriebssystem erfolgt.

Voreinstellung ist: **Deaktiviert**.

Die Option definiert, ob die Maschine automatisch neu gestartet wird, wenn das für die Wiederherstellung erforderlich ist. Dies ist beispielsweise der Fall, wenn ein Volume wiederhergestellt werden muss, welches vom Betriebssystem gesperrt wird.

Nach Abschluss der Wiederherstellung die Maschine automatisch neu starten

Diese Option ist wirksam, wenn Sie ein Boot-Medium gestartet haben und mit diesem arbeiten.

Voreinstellung ist: **Deaktiviert**.

Diese Option ermöglicht den Neustart der Maschine in das wiederhergestellte Betriebssystem ohne weitere Aktion eines Benutzers.

SID nach Wiederherstellung ändern

Diese Option ist nicht wirksam, wenn die Wiederherstellung zu einer virtuellen Maschine mit dem Acronis Backup & Recovery 11.5 Agenten für ESX/ESXi oder dem Acronis Backup & Recovery 11.5 Agenten für Hyper-V durchgeführt wird.

Voreinstellung ist: **Deaktiviert**.

Acronis Backup & Recovery 11.5 kann für das wiederhergestellte System einen eindeutigen Security Identifier (SID) generieren. Sie benötigen keinen neuen SID, wenn Sie das System auf der gleichen Maschine wiederherstellen, von der das Image erstellt wurde – oder wenn Sie ein Duplikat erstellen, welches das alte System ablöst. Generieren Sie einen neuen SID, wenn das ursprüngliche und das wiederhergestellte System gleichzeitig in einer Arbeitsgruppe oder Domain arbeiten werden.

5.7.2 Fehlerbehandlung

Diese Optionen sind für Windows, Linux-Betriebssysteme und das Boot-Medium wirksam.

Diese Optionen ermöglichen Ihnen vorzugeben, wie auftretende Fehler beim Recovery behandelt werden.

Während der Durchführung keine Meldungen bzw. Dialoge zeigen (stiller Modus)

Voreinstellung ist: **Deaktiviert**.

Wenn der stille Modus eingeschaltet ist, kann das Programm Situationen automatisch behandeln, die einen Benutzereingriff erfordern, falls das möglich ist. Falls eine Aktion nicht ohne Benutzereingriff fortfahren kann, wird sie fehlschlagen. Detaillierte Informationen über die Aktion, einschließlich eventueller Fehler, finden Sie im Log der Aktion.

Bei Fehler erneut versuchen

Voreinstellung ist: **Aktiviert**. **Zahl der Versuche: 30. Abstand zwischen Versuchen: 30 Sekunden.**

Wenn ein behebbarer Fehler auftritt, versucht das Programm, die erfolglose Aktion erneut durchzuführen. Sie können das Zeitintervall und die Anzahl der Versuche einstellen. Die Versuche werden aufgegeben, wenn entweder die Aktion erfolgreich ist ODER die angegebene Zahl der Versuche erreicht ist, je nachdem, was zuerst eintritt.

Wenn der Speicherort im Netzwerk nicht verfügbar oder erreichbar ist, wird die Anwendung versuchen, den Ort alle 30 Sekunden erneut zu erreichen, aber nur fünf Mal. Die Versuche werden aufgegeben, wenn entweder die Verbindung gelingt ODER die angegebene Zahl der Versuche erreicht ist, je nachdem, was zuerst eintritt.

5.7.3 Ereignisverfolgung

Es ist möglich, die von den Recovery-Aktionen auf verwalteten Maschinen erstellten Logs in die Ereignisanzeige von Windows zu duplizieren oder an spezifizierte SNMP-Manager zu senden.

5.7.3.1 SNMP-Benachrichtigungen

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar, wenn Sie ein Boot-Medium gestartet haben und mit diesem arbeiten.

Diese Option definiert, ob Agenten auf verwalteten Maschinen Log-Ereignisse von Recovery-Aktionen zu spezifizierten Simple Network Management Protocol (SNMP)-Managern schicken. Sie können die Arten der Ereignisse wählen, die geschickt werden.

Zu weiteren Informationen über die Verwendung von SNMP mit Acronis Backup & Recovery 11.5 siehe „Unterstützung für SNMP (S. 56)“.

Voreinstellung ist: **Einstellungen benutzen, die in den Maschinen-Optionen definiert sind.**

So wählen Sie, ob Ereignisse von Recovery-Aktionen an SNMP-Manager geschickt werden:

Wählen Sie eine der folgenden Optionen:

- **Einstellungen benutzen, die in den Optionen für die Maschine definiert sind** – für die Benutzung der Einstellungen, die in den Optionen für die Maschine spezifiziert sind. Weitere Informationen finden Sie bei Maschinen-Optionen.
- **SNMP-Benachrichtigungen über Ereignisse von Recovery-Aktionen einzeln senden** – für das Senden von SNMP-Benachrichtigungen mit den Ereignissen bei Recovery-Aktionen an spezifizierte SNMP-Manager.

    - **Ereignisse, die übermittelt werden** – Auswahl der Ereignistypen, die gesendet werden: **Alle Ereignisse**, **Fehler und Warnungen** oder **Nur Fehler**.
    - **Server-Name/IP** – Eintragen des Namens oder der IP-Adresse des Hosts mit der SNMP-Verwaltungsanwendung, an die die Meldungen gesendet werden.
    - **Community** – Eintragen des Namens der SNMP-Community, zu der der Host mit der SNMP-Verwaltungsanwendung und die sendende Maschine gehören. Die typische Community ist 'Public'.

  Klicken Sie auf **Testnachricht senden**, um die Richtigkeit der Einstellungen zu prüfen.
- **Keine SNMP-Benachrichtigungen senden** – Einstellung, um das Versenden von Ereignissen über Recovery-Aktionen an SNMP-Manager unwirksam zu machen.

5.7.3.2 Ereignisanzeige von Windows

Diese Option ist nur wirksam in Windows-Betriebssystemen.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Diese Option definiert, ob Agenten auf verwalteten Maschinen die Ereignisse der Recovery-Aktionen in der Windows Ereignisanzeige (Unterpunkt Anwendungen) aufzeichnen müssen (um die Ereignisanzeige zu sehen, führen Sie **eventvwr.exe** aus oder den Befehl **Systemsteuerung -> Verwaltung -> Ereignisanzeige**). Sie können die Ereignisse filtern, die geloggt werden.

Voreinstellung ist: **Einstellungen benutzen, die in den Optionen für die Maschine definiert sind.**

Wählen Sie, ob Ereigniseinträge der Recovery-Aktionen an die Ereignisanzeige von Windows übergeben werden.

Wählen Sie eine der nachfolgenden Varianten:

- **Einstellungen benutzen, die in den Optionen für die Maschine definiert sind** – für die Benutzung der Einstellungen, die in den Optionen für die Maschine spezifiziert sind. Weitere Informationen bei Optionen der Maschine.
- **Folgende Ereignisse protokollieren** – für das Loggen der Ereignisse der Recovery-Aktionen in der Ereignisanzeige. Arten der Ereignisse, die geloggt werden:
    - **Alle Ereignisse** – loggt alle Ereignisse (Informationen, Warnungen und Fehler)
    - **Fehler und Warnungen**
    - **Nur Fehler**
- **Nicht protokollieren** – für das Ausschalten der Protokollierung der Ereignisse der Recovery-Aktionen in der Ereignisanzeige.

5.7.4 Sicherheit auf Dateiebene

Diese Option ist nur für Wiederherstellungen von Windows-Dateien auf Dateiebene wirksam.

Diese Option definiert, ob die NTFS-Zugriffsrechte für Dateien zusammen mit den Dateien wiederhergestellt werden.

Voreinstellung ist: **Dateien mit ihren Sicherheitseinstellungen wiederherstellen**.

Wenn die NTFS-Zugriffsrechte auf die Dateien während des Backups (S. 127) erhalten wurden, können Sie wählen, ob Sie die Zugriffsrechte wiederherstellen oder ob Sie die Erlaubnis erteilen, dass die Dateien die NTFS-Zugriffsrechte vom Ordner erben, in den sie wiederhergestellt werden.

5.7.5 Mount-Punkte

Diese Option ist nur unter Windows zur Wiederherstellung von Daten aus einem dateibasierten Backup wirksam.

Aktivieren Sie die Option **Mount-Punkte**, um Dateien und Ordner wiederherzustellen, die auf gemounteten Volumes gespeichert waren und mit aktivierter Option **Mount-Punkte** gesichert wurden. Weitere Details zum Backup von gemounteten Volumes oder freigegebenen Cluster-Volumes finden Sie unter Mount-Punkte (S. 130).

Voreinstellung ist: **Deaktiviert**.

Diese Option ist nur wirksam, wenn Sie einen Ordner als Backup-Quelle auswählen, der in der Verzeichnishierarchie höher als der Mount-Punkt liegt. Wenn Sie einen Ordner innerhalb des Mount-Punktes oder den Mount-Punkt selbst für eine Recovery-Aktion wählen, werden die gewählten Elemente unabhängig vom Wert der Option '**Mount-Punkte**' wiederhergestellt.

Beachten Sie, dass für den Fall, dass das Volume zum Recovery-Zeitpunkt nicht gemountet ist, die Daten direkt zu demjenigen Ordner wiederhergestellt werden, der zum Backup-Zeitpunkt der Mount-Punkt war.

5.7.6 Benachrichtigungen

Acronis Backup & Recovery 11.5 kann Sie über den Abschluss eines Backups per E-Mail oder Windows Nachrichtendienst (WinPopup, nur bei Windows XP) benachrichtigen.

5.7.6.1 E-Mail

Diese Option ist für Windows- und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar, wenn Sie ein Boot-Medium gestartet haben und mit diesem arbeiten.

Die Option ermöglicht Ihnen den Erhalt von E-Mail-Benachrichtigungen über den erfolgreichen Abschluss von Recovery-Tasks, über Fehler oder wenn ein Benutzereingriff erforderlich ist.

Voreinstellung ist: **Deaktiviert**.

So konfigurieren Sie eine E-Mail-Benachrichtigung

1. Aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigung schicken**, um die entsprechende Funktion zu aktivieren.
2. Aktivieren Sie unter **E-Mail-Benachrichtigungen schicken** die entsprechenden Kontrollkästchen folgendermaßen:
   - **Wenn die Wiederherstellung erfolgreich abgeschlossen wurde**.
   - **Wenn die Wiederherstellung fehlschlägt**.
   - **Wenn Benutzereingriff erforderlich ist**.
3. Geben Sie die E-Mail-Adresse des Ziels im Feld **E-Mail-Adressen** ein. Sie können auch mehrere, per Semikolon getrennte Adressen eingeben.
4. Geben Sie im Feld **Betreff** eine Beschreibung für die Benachrichtigung ein.

   Die Betreffzeile kann gewöhnlichen Text und eine oder mehrere Variablen enthalten. In den empfangenen E-Mail-Nachrichten wird jede Variable dann durch den zum Zeitpunkt der Task-Ausführung vorliegenden Wert ersetzt. Folgende Variablen werden unterstützt:
   - **%description%**

Bei einer unter Windows laufenden Maschine wird die Variable **%description%** durch einen Text ersetzt, der dem Feld **Computerbeschreibung** der jeweiligen Maschine entspricht. Um den Text spezifizieren zu können, können Sie entweder zu **Systemsteuerung –> System** gehen oder folgenden Befehl als Administrator ausführen:

```
net config server /srvcomment:<text>
```

Bei einer unter Linux laufenden Maschine wird die Variable **%description%** durch einen leeren String ("") ersetzt.

- **%subject%**

  Die Variable **%subject%** wird in folgenden Ausdruck umgewandelt: *Task <Task-Name> <Task-Ergebnis> auf Maschine <Maschinenname>.*

5. Geben Sie im Feld **SMTP-Server** den Namen des ausgehenden Mail-Servers (SMTP) ein.
6. Legen Sie im Feld **Port** die Port-Nummer des ausgehenden Mail-Servers fest. Standardmäßig ist der Port auf **25** gesetzt.
7. Sollte der ausgehende Mail-Server eine Authentifizierung benötigen, dann geben Sie den **Benutzernamen** und das **Kennwort** vom E-Mail-Konto des Senders ein.

   Sollte der SMTP-Server keine Authentifizierung benötigen, dann lassen Sie die Felder **Benutzername** und **Kennwort** einfach leer. Falls Sie nicht sicher sind, ob Ihr SMTP-Server eine Authentifizierung erfordert, dann kontaktieren Sie Ihren Netzwerk-Administrator oder bitten Sie Ihren E-Mail-Dienstanbieter um Hilfe.
8. Klicken Sie auf **Erweiterte E-Mail-Parameter...**, um weitere E-Mail-Parameter folgendermaßen zu konfigurieren:

   a. **Von** – geben Sie den Namen des Absenders an. Falls Sie das Feld leer lassen, dann enthalten die Nachrichten im Feld **Von** das E-Mail-Konto des Senders.

   b. **Verschlüsselung verwenden** – Sie können sich für eine verschlüsselte Verbindung zum Mail-Server entscheiden. Zur Auswahl stehen die Verschlüsselungstypen SSL und TLS.

   c. Einige Internetdienstanbieter verlangen eine Authentifizierung am Posteingangsserver, bevor das Verschicken von Nachrichten erlaubt wird. Wenn das bei Ihnen zutrifft, aktivieren Sie das Kontrollkästchen **Anmeldung beim Posteingangsserver**, um einen POP3-Server zu aktivieren und seine Einstellungen einzurichten:

      - **Posteingangsserver (POP3)** – geben Sie den Namen des POP3-Servers an.
      - **Port** – bestimmt den Port des POP3-Servers. Standardmäßig ist der Port auf **110** gesetzt.
      - **Benutzername** und **Kennwort** für den eingehenden Mail-Server.

   d. Klicken Sie auf **OK**.
9. Klicken Sie auf **Test-Mail senden**, um zu überprüfen, ob die E-Mail-Benachrichtigungen mit den spezifizierten Einstellungen korrekt funktionieren.

5.7.6.2 Nachrichtendienst (WinPopup)

Diese Option ist für die Betriebssysteme Windows XP, Windows Server 2003 und Linux wirksam. Windows Vista und spätere Versionen von Windows unterstützen den Nachrichtendienst nicht mehr.

Diese Option ist nicht verfügbar, wenn Sie ein Boot-Medium gestartet haben und mit diesem arbeiten.

Die Option ermöglicht Ihnen den Erhalt von WinPopup-Benachrichtigungen über eine erfolgreiche Vollendung von Recovery-Tasks, über Fehler oder über erforderliche Handlungen.

Voreinstellung ist: **Deaktiviert.**

Vor Konfiguration der WinPopup-Benachrichtung sollten Sie sicherstellen, dass der Nachrichtendienst von Windows XP auf beiden Maschinen (die Task ausführende und die Nachrichten empfangende Maschine) gestartet ist.

Der Nachrichtendienst ist bei Windows XP SP2+ und Windows Server 2003/2003 R2 standardmäßig deaktiviert. Ändern Sie den **Starttyp** auf **Automatisch** und starten Sie den Dienst dann neu.

So konfigurieren Sie WinPopup-Benachrichtigungen:

1. Aktivieren Sie das Kontrollkästchen **WinPopup-Benachrichtigung schicken**.
2. Geben Sie in das Feld **Maschinenname** den Namen der Maschine ein, an die die Benachrichtigungen verschickt werden. Mehrere Namen werden nicht unterstützt.
3. Aktivieren Sie unter **Benachrichtigungen senden** die Kontrollkästchen folgendermaßen:
   - **Wenn die Wiederherstellung erfolgreich abgeschlossen wurde** – damit eine Benachrichtigung gesendet wird, wenn der Recovery-Task erfolgreich abgeschlossen wurde
   - **Wenn die Wiederherstellung fehlschlägt** – um eine Benachrichtigung abzuschicken, wenn der Wiederherstellungstask fehlgeschlagen ist.
   - **Wenn Benutzereingriff erforderlich ist** – zum Versenden einer Benachrichtigung, wenn während der Aktion das Eingreifen des Benutzers erforderlich ist.
4. Klicken Sie auf **WinPopup-Testnachricht senden**, um die Richtigkeit der Einstellungen zu prüfen.

5.7.7 Vor-/Nach-Befehle

Diese Option ist für Windows-, Linux-Betriebssysteme und das PE-Boot-Medium wirksam.

Diese Option ermöglicht die Definition von Befehlen, die automatisch vor oder nach der Datenwiederherstellung durchgeführt werden.

So benutzen Sie diese Vor- bzw. Nach-Befehle:

- Starten Sie den Befehl **Checkdisk**, damit logische Fehler im Dateisystem, physikalische Fehler oder fehlerhafte Sektoren vor Beginn oder nach Ende der Recovery-Aktion gefunden und behoben werden.

Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. „pause“).

Ein 'Nach-Recovery'-Befehl wird nicht ausgeführt, wenn die Wiederherstellung einen Neustart benötigt bzw. ausführt.

So spezifizieren Sie Vor-/Nach-Befehle

1. Sie aktivieren Vor-/Nach-Befehle mit Hilfe der folgenden Optionen:
   - **Vor Recovery ausführen**
   - **Nach Recovery ausführen**
2. Wählen Sie aus den nachfolgenden Varianten:
   - Klicken Sie auf **Bearbeiten**, um einen neuen Befehl oder eine Stapelverarbeitungsdatei zu spezifizieren.
   - Wählen Sie einen existierenden Befehl oder eine Stapelverarbeitungsdatei aus der Dropdown-Liste.
3. Klicken Sie auf **OK**.

5.7.7.1 Befehl vor Recovery

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die vor dem Start der Wiederherstellung ausgeführt wird

1. Tragen Sie im Eingabefeld **Befehl** einen Befehl ein oder suchen Sie eine vorbereitete Stapelverarbeitungsdatei. Das Programm unterstützt keine interaktiven Befehle, d.h. Befehle, die eine Reaktion des Benutzers erfordern (wie z.B. „pause“).
2. Spezifizieren Sie im Eingabefeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden.
3. Tragen Sie Argumente für die Befehlsausführung in das Feld **Argumente** ein, wenn das erforderlich ist.
4. Wählen Sie in der unteren Tabelle die passenden Optionen, abhängig vom Ergebnis, das Sie erreichen wollen.
5. Klicken Sie auf **Befehl testen**, um zu prüfen, ob der Befehl korrekt funktioniert.

Kontrollkästchen	**Auswahl**			
Task scheitern lassen, wenn die Befehlsausführung fehlschlägt*	Ausgewählt	Deaktiviert	Ausgewählt	Deaktiviert
Keine Wiederherstellung bis die Befehlsausführung abgeschlossen ist	Ausgewählt	Ausgewählt	Deaktiviert	Deaktiviert
Ergebnis				
	Voreinstellung Recovery nur durchführen, nachdem der Befehl erfolgreich ausgeführt wurde. Task scheitern lassen, wenn die Befehlsausführung fehlschlägt.	Recovery nach Befehlsausführung fortsetzen, unabhängig vom Erfolg oder Misserfolg der Ausführung.	Nicht verfügbar	Recovery gleichzeitig mit Befehlsausführung durchführen, unabhängig vom Ergebnis der Befehlssausführung.

* Ein Befehl wird als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist.

5.7.7.2 Befehl nach Recovery

So spezifizieren Sie einen Befehl bzw. eine Stapelverarbeitungsdatei, die ausgeführt wird, wenn die Wiederherstellung vollständig ist

1. Tragen Sie im Eingabefeld **Befehl** ein Kommando ein oder suchen Sie eine vorbereitete Stapelverarbeitungsdatei.
2. Spezifizieren Sie im Eingabeld **Arbeitsverzeichnis** einen Pfad zu einem Verzeichnis, in dem der Befehl bzw. die Stapelverarbeitungsdatei durchgeführt werden.
3. Tragen Sie, sofern erforderlich, in das Feld **Argumente** entsprechende Parameter für die Befehlsausführung ein.
4. Aktivieren Sie das Kontrollkästchen **Task scheitern lassen, wenn die Befehlsausführung fehlschlägt**, sofern eine erfolgreiche Ausführung des Befehls wichtig für Sie ist. Der Befehl wird

als 'fehlgeschlagen' betrachtet, wenn sein Exit-Code ungleich Null ist. Falls die Befehlsausführung fehlschlägt, wird das auch das Ergebnis der Task-Aktion auf 'fehlgeschlagen' gesetzt.

Wenn das Kontrollkästchen nicht ausgewählt ist, dann hat das Ergebnis der Befehlsausführung keinen Einfluss auf Erfolg oder Misserfolg des Tasks. Sie können das Ergebnis der Befehlsausführung durch Einsicht in die Anzeige **Log** verfolgen.

5. Klicken Sie auf **Befehl testen**, um zu prüfen, ob der Befehl korrekt funktioniert.

Ein 'Nach-Recovery'-Befehl wird nicht ausgeführt, wenn die Wiederherstellung einen Neustart benötigt bzw. ausführt.

5.7.8 Recovery-Priorität

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Die Priorität eines jeden Prozesses, der in einem System läuft, hängt vom Grad der CPU-Benutzung und der Systemressourcen ab, die dem Prozess zugeordnet werden. Das Herabsetzen der Recovery-Priorität wird mehr Ressourcen für andere Anwendungen freisetzen. Das Heraufsetzen der Recovery-Priorität kann den Wiederherstellungsprozess beschleunigen, indem z.B. CPU-Ressourcen von anderen gleichzeitig laufenden Prozessen abgezogen werden. Der Effekt ist aber abhängig von der totalen CPU-Auslastung und anderen Faktoren wie der Schreibgeschwindigkeit der Festplatte oder dem Datenverkehr im Netzwerk.

Voreinstellung ist: **Normal.**

So spezifizieren Sie die Priorität des Recovery-Prozesses

Wählen Sie eine der nachfolgenden Varianten:

- **Niedrig** – minimiert die durch den Recovery-Prozess verwendeten Ressourcen und belässt mehr Ressourcen für andere Prozesse, die auf der Maschine laufen.
- **Normal** – führt den Recovery-Prozess mit normaler Geschwindigkeit aus und teilt die verfügbaren Ressourcen mit anderen Prozessen.
- **Hoch** – maximiert die Geschwindigkeit des Recovery-Prozesses und zieht Ressourcen von anderen Prozessen ab.

6 Konvertierung zu einer virtuellen Maschine

Acronis Backup & Recovery 11.5 ermöglicht mehrere Möglichkeiten, ein Laufwerk-Backup in eine virtuelle Maschine zu konvertieren. Dieser Abschnitt soll Ihnen helfen, die Methode zu finden, die Ihren Bedürfnissen am besten entspricht – und stellt Schritt-für-Schritt-Anleitungen zur Konvertierung bereit.

6.1 Konvertierungsmethoden

Sie können, abhängig von Ihren Anforderungen, zwischen folgenden Konvertierungsmethoden wählen:

a) **Die Konvertierung zum Teil eines Backup-Plans machen**

Zeitpunkt der Verwendung.

- Falls Sie möchten, dass das Backup und die Konvertierung nach Planung ausgeführt werden. Das hilft Ihnen, einen auf Standby stehenden virtuellen Server aufrechtzuerhalten, falls Ihr physikalischer Server ausfällt.
- Falls Sie die resultierenden Einstellungen der virtuellen Maschine nicht anpassen müssen.

Art der Durchführung. Aktivieren Sie bei Erstellung eines Backup-Plans (S. 58) die Funktion zur Konvertierung eines Backups zu einer virtuellen Maschine (S. 192).

b) **Wiederherstellung der gesicherten Laufwerke oder Volumes mit dem Ziel 'Neue virtuelle Maschine'**

Zeitpunkt der Verwendung.

- Falls Sie die Konvertierung bei Bedarf einmalig oder gelegentlich durchführen wollen.
- Falls Sie eine verlustfreie Migration von 'Physikalisch zu virtuell' durchführen wollen. Booten Sie in diesem Fall die ursprüngliche Maschine mit einem bootfähigen Medium, erstellen Sie ein Backup der Maschine im Offline-Stadium und stellen Sie die Maschine dann direkt aus dem resultierenden Backup wieder her.
- Falls Sie die resultierenden Einstellungen der virtuellen Maschine anpassen müssen. Sie können Laufwerke hinzufügen oder entfernen, den Provisioning-Modus für Laufwerke wählen, die Größe und den Speicherort von Volumes auf den Laufwerken ändern und mehr.

Art der Durchführung. Folgen Sie den im Abschnitt 'Wiederherstellung mit dem Ziel 'Neue virtuelle Maschine' (S. 196)' beschriebenen Schritten.

c) **Wiederherstellung der gesicherten Laufwerke oder Volumes unter Verwendung eines bootfähigen Mediums zu einer manuell erstellten virtuellen Maschine**

Zeitpunkt der Verwendung.

- Falls Sie eine Maschine direkt auf einem Virtualisierungsserver erstellen wollen, statt sie zu importieren.

  Tipp: Mit dem Agenten für ESX(i) oder dem Agenten für Hyper-V kann eine virtuelle Maschine direkt auf einem entsprechenden Virtualisierungsserver mit den Methoden (a) und (b) erstellt werden.
- Falls Sie dynamische Volumes auf einer Windows-Maschine neu erstellen müssen.
- Falls Sie logische Volumes oder ein Software-RAID auf einer Linux-Maschine neu erstellen müssen.

Art der Durchführung. Folgen Sie den im Abschnitt 'Wiederherstellung zu einer manuell erstellten virtuellen Maschine (S. 199)' beschriebenen Schritten.

6.2 Konvertierung zu einer automatisch erstellten virtuellen Maschine

Dieser Abschnitt beschreibt die Konvertierungsmethoden (S. 190), mit denen Acronis Backup & Recovery 11.5 eine neue virtuelle Maschine automatisch erstellt:

- Während einer Konvertierung, die Teil eines Backup-Plans ist (S. 192), erstellt die Software die virtuelle Maschine zusätzlich zur Erstellung des Backups. Die virtuelle Maschine hat dieselbe Konfiguration wie die ursprüngliche Maschine.
- Während einer Wiederherstellung mit dem Ziel 'Neue virtuelle Maschine' (S. 196) erstellt die Software die virtuelle Maschine von einem Backup, welches bereits vorliegt. Sie können die Konfiguration der virtuellen Maschine ändern.

Acronis Backup & Recovery 11.5 kann, abhängig von dem die Konvertierung durchführenden Agenten, eine virtuelle Maschine mit jedem der folgenden Formate erstellen:

Agent für Windows, Agent für Linux

- VMware Workstation
- Microsoft Virtual PC (einschließlich Windows Virtual PC)
- Citrix XenServer OVA (nur während einer Wiederherstellung zum Ziel 'Neue virtuelle Maschine')
- Kernel-based Virtual Machine
- Red Hat Enterprise Virtualization (RAW-Format)

Agent für ESX(i)

- VMware ESX(i)

Agent für Hyper-V

- Microsoft Hyper-V

6.2.1 Überlegungen vor der Konvertierung

Konvertieren einer UEFI-basierten Maschine

Virtuellen Maschinen, die UEFI (Unified Extensible Firmware Interface) verwenden, werden derzeit nur in VMware ESXi 5 unterstützt. Falls es sich bei der als Ziel dienenden Virtualisierungsplattform um ESXi 5 handeln, dann erstellt Acronis Backup & Recovery 11.5 eine UEFI-basierte Maschine. Anderenfalls wird die resultierende Maschine die BIOS-Boot-Firmware verwenden.

Acronis Backup & Recovery 11.5 passt den Windows-Boot-Modus an die BIOS-Boot-Firmware an und stellt so sicher, dass Windows bootfähig bleibt.

Bei Linux-Betriebssystemen wird eine Änderung des Boot-Modus von UEFI zu BIOS nicht unterstützt. Stellen Sie bei Konvertierung einer unter Linux laufenden, UEFI-basierten Maschine sicher, dass diese GRUB Version 1 verwendet und dass die Zielvirtualisierungsplattform ESXi 5 ist. Weitere Details finden Sie im Abschnitt 'Unterstützung für UEFI-basierte Maschinen (S. 53)'.

Logische und dynamische Volumes

Die resultierende Maschine wird Basis-Volumes haben, selbst wenn im Backup eine logische Linux-Volume-Struktur vorliegt. Dasselbe gilt für dynamische, unter Windows verwendete Volumes. Falls Sie auf der Maschine logische oder dynamische Volumes neu erstellen wollen, dann führen Sie die Konvertierung so durch, wie im Abschnitt 'Wiederherstellung zu einer manuell erstellten virtuellen Maschine (S. 199)' beschrieben.

Reaktivierung eines benutzerdefinierten Loaders (Custom Loader)

- Die Laufwerksschnittstellen können während der Konvertierung geändert werden, etwa als Ergebnis der Migration zu einer anderen Plattform oder wegen manueller Anpassung. Die Software stellt die Systemlaufwerkschnittstelle so ein, dass sie der Standardschnittstelle der neuen Plattform entspricht. Für VMWare ist die Standardschnittstelle SCSI, für andere unterstützte Plattformen ist sie IDE. Wenn sich die Schnittstelle des Systemlaufwerks ändert, dann ändert sich auch der Name des Boot-Gerätes; der Bootloader verwendet jedoch weiterhin den alten Namen.
- Eine Konvertierung von logischen Volumes zu solchen vom Typ 'Basis' kann außerdem bewirken, dass das System nicht mehr booten kann.

Falls die Maschine einen benutzerdefinierten Boot-Loader (Custom Loader) verwendet, müssen Sie diesen daher evtl. so konfigurieren, dass er auf die neuen Geräte verweist und den Loader reaktivieren. Eine Konfiguration von GRUB ist normalerweise nicht notwendig, weil Acronis Backup & Recovery 11.5 dies automatisch durchführt. Sollte es doch notwendig sein, dann verwenden Sie die im Abschnitt 'So reaktivieren Sie GRUB und ändern seine Konfiguration (S. 177)' beschriebene Prozedur.

Weitere Überlegungen zur Konvertierung von physikalischen zu virtuellen Maschinen finden Sie im Dokument 'Backups von virtuellen Maschinen'.

6.2.2 Regelmäßige Konvertierung zu einer virtuellen Maschine einrichten

Sie können bei Erstellung eines Backup-Plans (S. 58) einstellen, dass Laufwerk- oder Volume-Backups regelmäßig zu einer virtuellen Maschine konvertiert werden. Durch Einrichten einer regelmäßigen Konvertierung erhalten Sie eine Kopie Ihres Servers oder Ihrer Workstation in Form einer virtuellen Maschine, die sofort einsatzbereit ist, falls die ursprüngliche Maschine ausfallen sollte.

Einschränkungen

- Eine Backup-Konvertierung ist von folgenden Speicherorten aus nicht verfügbar: CDs, DVDs, Blu-Ray-Discs, Bandgeräte und der Acronis Online Backup Storage.
- Die Konvertierung zu einer virtuellen Maschine vom Typ 'Citrix XenServer' ist als Bestandteil eines Backup-Plans nicht verfügbar. Verwenden Sie als Alternative die Methoden (b) und (c), wie im Abschnitt 'Konvertierungsmethoden (S. 190)' beschrieben.
- Microsoft Virtual PC unterstützt keine virtuellen Laufwerke, die größer als 127 GB sind. Während der Konvertierung zu einer Virtual PC-Maschine wird die Größe eines jeden Laufwerks, welches 127 GB überschreitet, auf diesen Wert verkleinert. Sollte die Größenanpassung des Laufwerks nicht möglich sein, schlägt die Konvertierung fehl. Sollten Sie größere virtuelle Laufwerke benötigen, um diese an eine Hyper-V-Maschine anzubinden, dann verwenden Sie die unter 'Konvertierungsmethoden (S. 190)' beschriebenen Methoden (b) und (c).

6.2.2.1 Konvertierungseinstellungen

Die Informationen in diesem Abschnitt sollen Ihnen helfen, die passenden Konvertierungseinstellungen vorzunehmen.

Die Einstellungen werden im Bereich **Zu virtueller Maschine konvertieren** der Seite **Backup-Plan erstellen** spezifiziert.

Zu virtueller Maschine konvertieren

Konvertierungsquelle

Falls Sie Backups zu anderen Speicherorten kopieren oder verschieben (S. 104), dann wählen Sie den Speicherort, von dem das Backup genommen werden soll.
Konvertierungsspeicherorte, die nicht verfügbar (S. 192) sind (wie der Acronis Online Backup Storage) werden nicht aufgelistet.

Standardmäßig werden Konvertierungen vom primären Speicherort aus durchgeführt.

Konvertierungszeitpunkt

Spezifizieren Sie, abhängig vom gewählten Backup-Schema, ob jedes vollständige, inkrementelle oder differentielle Backup konvertiert werden soll oder das jeweils letzte nach Planung erstellte Backup. Spezifizieren Sie bei Bedarf die **Konvertierungsplanung** (S. 193).

Ziel-Host... (S. 194)

Bestimmen Sie den Typ und Speicherort der resultierenden virtuellen Maschine. Die verfügbaren Optionen hängen von dem Agenten ab, der die Konvertierung durchführt. Das kann der Agent sein, der (standardmäßig) das Backup durchführt oder ein Agent, der auf einer anderen Maschine installiert ist. Im letzteren Fall muss das Archiv an einem gemeinsam nutzbaren Ort gespeichert werden, z.B. einem Netzwerkordner oder einem verwalteten Depot, damit die andere Maschine auf das Archiv zugreifen kann.

Klicken Sie zur Spezifikation eines anderen Agenten auf **Ändern** und wählen Sie eine Maschine, auf der ein Agent für ESX(i), ein Agent für Hyper-V, ein Agent für Windows oder ein Agent für Linux installiert ist.

Storage

Wählen Sie den Storage auf dem Virtualisierungsserver oder den Ordner, wo die Dateien der virtuellen Maschine gespeichert werden sollen.

Resultierende VMs

Spezifizieren Sie den Namen der virtuellen Maschine. Die vorgegebene Bezeichnung ist **Backup_von_[Maschinenname]**. Sie können dem Namen weitere Variablen hinzufügen. Folgende Vorlagen werden unterstützt:

[Plan-Name]
[Maschinenname]
[Virtueller Host-Name]
[Name der virtuellen Maschine]
[Virtualisierungsservertyp]

Ordner auf dem VMware vCenter

Wenn der Management Server mit dem vCenter Server integriert ist, erscheinen die resultierenden Maschinen im Ordner **Acronis Backups** auf dem vCenter. Sie können einen Unterordner für die Maschinen spezifizieren, die aus der Ausführung des Plans resultieren.

6.2.2.2 Eine Konvertierungsplanung einrichten

Ein bei Ausführung eines Backup-Plans erstelltes Laufwerk-Backup (S. 489) kann sofort oder per Planung zu einer virtuellen Maschine konvertiert werden – oder durch eine Kombination beider Methoden.

Der Konvertierungstask wird auf der zu sichernden Maschine erstellt und verwendet die Zeiteinstellungen der Maschine. Falls der Agent, der die Maschine sichert, außerhalb von dieser installiert ist (ist der Fall, wenn virtuelle ESX(i)- oder Hyper-V-Maschinen auf Hypervisor-Ebene gesichert werden), dann wird der Task auf der Maschine erstellt, auf der sich der Agent befindet.

Die virtuelle Zielmaschine muss zum Zeitpunkt der Konvertierung heruntergefahren sein, sonst schlägt der Konvertierungstask fehl. Sollte das passieren, dann können Sie den Konvertierungstask manuell neu starten, nachdem die betreffende Maschine ausgeschaltet wurde. Änderungen, die an der Maschine durchgeführt wurden, während sie eingeschaltet war, werden überschrieben.

6.2.2.3 Eine Maschine zur Durchführung von Konvertierungen wählen

Berücksichtigen Sie folgende Überlegungen.

Welcher Agent ist auf der Maschine installiert?

Typ und Speicherort der resultierenden virtuellen Maschine hängen von dem Agenten ab, der auf der gewählten Maschine vorliegt.

- Der **Agent für ESX(i)** ist auf der Maschine installiert

  Falls der Agent mehr als einen ESX(i)-Host verwaltet, dann können Sie den Host wählen, auf dem die virtuelle Maschine erstellt wird.

  Im Schritt **Storage** können Sie den Speicherort/-Typ wählen, wo die virtuelle Maschine erstellt wird.

  Als Ergebnis eines Backups erstellte virtuelle Maschinen können einem Backup-Plan nicht hinzugefügt werden. Sie erscheinen auf dem Management Server als 'nicht verwaltbar' oder erscheinen überhaupt nicht (falls keine Integration mit dem vCenter-Server aktiviert ist).
- Der **Agent für Hyper-V** ist auf der Maschine installiert

  Sie können eine virtuelle Maschine nur auf dem Hyper-V-Server erstellen.

  Im Schritt **Storage** können Sie den Pfad zur virtuellen Maschine wählen.

  Infolge eines Backups auf dem Server erstellte virtuelle Maschinen erscheinen nicht auf dem Management Server, weil solche Maschinen nicht dazu gedacht sind, per Backup gesichert zu werden.
- Der **Agent für Windows** oder der **Agent für Linux** sind auf der Maschine installiert

  Sie können den Typ der virtuellen Maschine wählen: VMware Workstation, Microsoft Virtual PC, Red Hat Kernel-based Virtual Machine (KVM) oder Red Hat Enterprise Virtualization (RHEV).

  Im Schritt **Storage** können Sie den Pfad zur virtuellen Maschine wählen.

Wie ist die Rechenleistung der Maschine?

Die Konvertierung belastet die CPU-Ressourcen der gewählten Maschine. Mehrere Konvertierungstasks werden auf dieser Maschine über eine Warteschlange abgearbeitet, deren vollständige Abarbeitung eine beträchtliche Zeit benötigen kann. Sie sollten dies berücksichtigen, wenn Sie einen zentralen Backup-Plan mit Konvertierung mehrerer Maschinen erstellen – oder wenn Sie mehrere lokale Backup-Pläne erstellen, die dieselbe Maschine zur Konvertierung verwenden.

Welcher Storage wird für die virtuellen Maschinen verwendet?

Netzwerkauslastung

Im Gegensatz zu üblichen Backups (tib-Dateien) werden die 'Virtuellen Maschinen'-Dateien unkomprimiert durch das Netzwerk übertragen. Aus Sicht der Netzwerkauslastung ist es daher am besten, ein SAN oder einen lokalen Storage für die Maschine zu verwenden, die die Konvertierung ausführt. Sie können jedoch kein lokales Laufwerk wählen, wenn die Konvertierung von derselben Maschine durchgeführt wird, die auch gesichert wird. Die Verwendung eines NAS macht ebenfalls Sinn.

Speicherplatz

Bei VMware, Hyper-V und Virtual PC werden die Laufwerke der resultierenden virtuellen Maschine so viel Speicherplatz wie die ursprünglichen Daten belegen. Bei einer angenommenen ursprünglichen Laufwerksgröße von 100 GB, von denen 10 GB mit Daten belegt sind, ergibt sich ein entsprechendes virtuelles Laufwerk von ebenfalls ca. 10 GB. VMware nennt dieses Format 'Thin Provisioning', Microsoft verwendet den Begriff 'Laufwerk mit dynamischer Erweiterung' (Dynamically Expanding Disk). Da der Speicherplatz nicht vorab zugeordnet wird, wird für den physikalischen Storage angenommen, dass er noch genügend freien Speicherplatz hat, damit die virtuellen Laufwerke auch noch an Größe zunehmen können.

Bei KVM oder RHEV werden die Laufwerke der resultierenden virtuellen Maschine das Raw-Format haben. Das bedeutet, dass die virtuelle Laufwerksgröße immer gleich zur ursprünglichen Laufwerkskapazität ist. Angenommen, die ursprüngliche Laufwerksgröße beträgt 100 GB, dann wird das korrespondierende virtuelle Laufwerk 100 GB belegen, selbst wenn das Laufwerk nur Daten von 10 GB speichert.

6.2.2.4 Wie die 'regelmäßige Konvertierung zu VM' arbeitet

Wie die wiederholte Konvertierung arbeitet, hängt davon ab, wo nach Ihrer Wahl die virtuelle Maschine erstellt werden soll.

- **Bei Auswahl, dass die virtuelle Maschine als ein Satz von Dateien gespeichert werden soll:** Erstellt jede Konvertierung die virtuelle Maschine von Grund aus neu.
- **Bei Auswahl, dass die virtuelle Maschine auf einem Virtualisierungsserver erstellt werden soll:** Aktualisiert die Software eine existierende virtuelle Maschine statt sie neu zu erstellen, wenn ein inkrementelles oder differentielles Backup konvertiert wird. Eine solche Konvertierung ist normalerweise schneller. Sie geht sparsamer mit Netzwerkverkehr und CPU-Ressourcen des Hosts um, der die Konvertierung durchführt. Falls eine virtuelle Maschine nicht aktualisiert werden kann, erstellt die Software auch diese von Grund auf neu.

Nachfolgend finden Sie eine genauere Beschreibung beider Fälle.

Bei Auswahl, dass die virtuelle Maschine als ein Satz von Dateien gespeichert werden soll

Als Folge der ersten Konvertierung wird eine neue virtuelle Maschine erstellt. Jede nachfolgende Konvertierung wird diese Maschine jeweils ganz neu erstellen. Zuerst wird die alte Maschine temporär umbenannt. Dann wird eine neue virtuelle Maschine erstellt, die den vorherigen Namen der alten Maschine hat. Sobald diese Aktion erfolgreich abgeschlossen wurde, wird die alte Maschine gelöscht. Wenn die Aktion fehlschlägt, wird die neue Maschine gelöscht und die alte Maschine erhält ihren früheren Namen zurück. Auf diese Art schließt die Konvertierung immer mit einer einzelnen Maschine ab. Jedoch wird während der Konvertierung zusätzlicher Speicherplatz benötigt, um die alte Maschine aufzunehmen.

Bei Auswahl, dass die virtuelle Maschine auf einem Virtualisierungsserver erstellt werden soll

Die erste Konvertierung erstellt eine ganz neue virtuelle Maschine. Jede nachfolgende Konvertierung arbeitet folgendermaßen:

- Falls es seit der letzten Konvertierung ein *Voll-Backup* gegeben hat, wird die virtuelle Maschine ganz neu erstellt (wie zuvor in diesem Abschnitt beschrieben).
- Anderenfalls wird die existierende virtuelle Maschine so aktualisiert, dass sie die Änderungen seit der letzten Konvertierung widerspiegelt. Wenn eine Aktualisierung (Update) nicht möglich ist

(beispielsweise, weil Sie die zwischenzeitlichen Snapshots gelöscht haben, siehe nachfolgend), wird die virtuelle Maschine ganz neu erstellt.

Zwischenzeitliche Snapshots

Um die virtuelle Maschine aktualisieren zu können, speichert die Software einige zwischenzeitliche Snapshots von ihr. Sie werden **Backup…** und **Replica…** genannt und sollten behalten werden. Nicht mehr benötigte Snapshots werden automatisch gelöscht.

Der jüngste **Replikat…**-Snapshot korrespondiert mit dem Ergebnis der letzten Konvertierung. Sie können zu diesem Snapshot zurückgehen, falls Sie die Maschine auf dieses Stadium zurücksetzen wollen – beispielsweise, weil Sie mit der Maschine gearbeitet haben und nun durchgeführte Änderungen verwerfen wollen.

Andere Snapshots sind nur zur internen Verwendung durch die Software.

6.2.3 Wiederherstellung mit dem Ziel 'Neue virtuelle Maschine'

Statt eine tib-Datei einfach nur zu einer virtuellen Laufwerksdatei zu konvertieren (was zusätzliche Aktionen für die Verfügbarkeit des virtuellen Laufwerks erforderlich machen würde), führt Acronis Backup & Recovery 11.5 die Konvertierung so aus, dass das betreffende Laufwerk-Backup in Form einer neuen, vollständig konfigurierten und betriebsbereiten virtuellen Maschine wiederhergestellt wird. Sie können bei der Vorbereitung der Recovery-Aktion die Konfiguration der virtuellen Maschine an Ihre speziellen Anforderungen anpassen.

Sie können mit dem **Acronis Backup & Recovery 11.5 Agenten für Windows** oder dem **Agenten für Linux** eine neue virtuelle Maschine in einem lokalen Ordner oder Netzwerkordner erstellen. Sie können die Maschine unter Verwendung der entsprechenden Virtualisierungssoftware starten oder die Dateien der Maschine für eine zukünftige Verwendung vorbereiten. Die folgende Tabelle fasst die verfügbaren virtuellen Maschinen-Formate und möglichen Aktionen zusammen, um die Maschine einem Virtualisierungsserver hinzuzufügen.

VM-Format	Weitere Aktion und zu verwendendes Tool	Zielvirtualisierungsplattform
VMware Workstation	Exportieren mit VMware Workstation; oder Konvertieren zu OVF mit dem VMware OVF-Toool > Deployment des OVF-Templates mit dem vSphere Client	ESX(i)
Microsoft Virtual PC*	Die VHD-Datei einer Hyper-V-Maschine hinzufügen	Hyper-V
Citrix XenServer OVA	Importieren mit dem Citrix XenCenter	XenServer
Kernel-based Virtual Machine (Raw-Format)	Verschieben der virtuellen Maschinen-Dateien zu einer unter Linux laufenden Maschine und Ausführung der virtuellen Maschine mit dem Virtual Machine Manager	-
Red Hat Enterprise Virtualization (RHEV) (Raw-Format)	Importieren mit dem RHEV-Manager	RHEV

*Microsoft Virtual PC unterstützt keine Laufwerke, die größer als 127 GB sind. Acronis ermöglicht Ihnen, eine Virtual PC-Maschine mit größeren Laufwerken zu erstellen, so dass Sie die Laufwerke an eine virtuelle Microsoft Hyper-V-Maschine anbinden können.

Sie können mit dem **Acronis Backup & Recovery 11.5 Agenten für Hyper-V** oder **Agenten für ESX(i)** eine neue virtuelle Maschine direkt auf dem entsprechenden Virtualisierungsserver erstellen.

6.2.3.1 Auszuführende Schritte

So führen Sie eine Wiederherstellung zu einer neuen virtuellen Maschine durch

1. Verbinden Sie die Konsole mit dem Management Server, mit einer Maschine, auf der ein Agent installiert ist oder mit einer Maschine, die mit einem bootfähigen Medium gestartet wurde.
2. Klicken Sie auf **Recovery**, um die Seite **Daten wiederherstellen** (S. 146) zu öffnen.
3. Klicken Sie auf **Daten wählen** (S. 147). Verwenden Sie die Registerlasche **Datenanzeige** oder **Archiv-Anzeige**, um die Laufwerke bzw. Volumes für die Konvertierung auszuwählen.
4. Wählen Sie unter **Recovery nach** das Element **Neue virtuelle Maschine**.
5. Klicken Sie auf **Durchsuchen**. Wählen Sie im Fenster **VM/VS-Auswahl** (S. 197) den resultierenden Typ der virtuellen Maschine oder den Virtualisierungsserver, auf dem die Maschine erstellt werden soll.
6. [Optional] Sie können bei **Storage** sehen oder wählen, wo die virtuelle Maschine erstellt wird.
7. [Optional] Sie können bei **Einstellungen der virtuellen Maschine** (S. 198) den Namen der neuen virtuellen Maschine, den 'Provisioning'-Laufwerksmodus, die Speicherzuteilung sowie andere Einstellungen ändern.

   Maschinen, die denselben Typ und denselben Namen haben, können nicht im selben Ordner erstellt werden. Wenn Sie eine Fehlermeldung erhalten, die durch identische Namen hervorgerufen wurde, dann ändern Sie entweder den VM-Namen oder den Pfad.

8. Das Ziellaufwerk für jedes der Quelllaufwerke bzw. Quell-Volumes und MBRs wird automatisch ausgewählt. Sie können die Ziellaufwerke bei Bedarf ändern.

   Unter Microsoft Virtual PC, wo sich der Loader des Betriebssystems auf Laufwerk 1 befindet, müssen Sie unbedingt dieses Laufwerk oder Volume wiederherstellen. Anderenfalls wird das Betriebssystem nicht booten. Das kann durch Ändern der Reihenfolge der Boot-Geräte im BIOS nicht repariert werden, weil Virtual PC diese Einstellungen ignoriert.

9. Geben Sie unter **Recovery-Zeitpunkt** an, wann der Recovery-Task beginnen soll.
10. [Optional] Überprüfen Sie bei **Task** die **Recovery-Optionen** und ändern Sie die Standardeinstellungen gegebenenfalls ab. Sie können bei **Recovery-Optionen –> VM-Energieverwaltung** spezifizieren, ob die neue virtuelle Maschine automatisch gestartet werden soll, nachdem die Wiederherstellung abgeschlossen wurde. Diese Option ist nur verfügbar, wenn die neue Maschine auf einem Virtualisierungsserver erstellt wird.
11. Klicken Sie auf **OK**. Wenn der Recovery-Task für einen späteren Zeitpunkt geplant ist, geben Sie die Anmeldedaten an, unter denen der Task ausgeführt wird.

Sie können in der Ansicht **Backup-Pläne und Tasks** das Stadium und den Fortschritt des Recovery-Tasks überprüfen.

6.2.3.2 Typ der virtuellen Maschine / Wahl des Virtualisierungsservers

Wählen Sie den resultierenden Typ der virtuellen Maschine oder den Virtualisierungsserver, auf dem die Maschine erstellt wird.

Die verfügbaren Optionen hängen von dem (den) Agent(en) ab, der (die) auf der Maschine installiert ist (sind), mit der die Konsole verbunden ist. Wenn die Konsole mit dem Management Server verbunden ist, können Sie jede registrierte Maschine wählen, die in der Lage ist, die erforderliche Aktion durchzuführen.

So bestimmen Sie den Virtualisierungsserver, auf dem die virtuelle Maschine erstellt wird

1. Wählen Sie die Option **Eine neue virtuelle Maschine auf dem Server erstellen**.

2. Wählen Sie im linken Teil des Fensters den Virtualisierungsserver. Verwenden Sie den rechten Fensterbereich, um Details über den gewählten Server einzusehen.

   [Nur, wenn die Konsole mit dem Management Server verbunden ist] Falls mehrere Agenten den ausgewählten ESX(i)-Host verwalten, können Sie den Agenten auswählen, der die Wiederherstellung durchführen soll. Wählen Sie zur Erreichung einer besseren Performance einen Agenten für ESX(i) (Virtuelle Appliance), der sich auf dem ESX(i) befindet. Falls kein Agent den ESX(i) verwaltet und die Funktion Automatisches Deployment aktiviert ist, dann wird der Agent für ESX(i) (Virtuelle Appliance) sofort bereitgestellt, nachdem Sie auf **OK** geklickt haben. Die Wiederherstellung wird von diesem Agenten durchgeführt. Er wird eine Lizenz in Anspruch nehmen.
3. Klicken Sie auf **OK**, um zur Seite **Daten wiederherstellen** zurückzukehren.

So wählen Sie den Typ der virtuellen Maschine

1. Wählen Sie die Option **Die virtuelle Maschine als eine Zusammenstellung von Dateien speichern**.
2. Wählen Sie im linken Teil des Fensters den Typ der virtuellen Maschine. Verwenden Sie den rechten Fensterbereich, um Details über den gewählten Typ der virtuellen Maschine einzusehen.

   [Nur, wenn die Konsole mit dem Management Server verbunden ist] Sie können die Maschine wählen, die die Wiederherstellung durchführen wird. Das kann jede registrierte Maschine sein, auf welcher der Agent für Windows oder der Agent für Linux installiert ist.
3. Klicken Sie auf **OK**, um zur Seite **Daten wiederherstellen** zurückzukehren.

6.2.3.3 Einstellungen der virtuellen Maschine

Sie können die nachfolgenden Einstellungen der virtuellen Maschinen konfigurieren.

Laufwerke

Anfangseinstellung: Die Zahl und Größe der Laufwerke der Quellmaschine.

Die Anzahl der Laufwerke ist üblicherweise gleich zu denen der Quellmaschine. Sie kann jedoch abweichen, wenn die Software weitere Laufwerke hinzufügen muss, um die Volumes der Quellmaschine aufzunehmen, weil das Virtualisierungsprodukt hier Limitierungen setzt. Sie können der Maschinen-Konfiguration weitere virtuelle Laufwerke hinzufügen oder in manchen Fällen das vorgeschlagene Laufwerk löschen.

Sie können beim Hinzufügen eines neuen virtuellen Laufwerkes zusammen mit seiner Schnittstelle und Kapazität auch das Format spezifizieren.

- **Format 'Thin' (Schlank).** Das Laufwerk belegt so viel Speicherplatz, wie es der Größe der gespeicherten Daten entspricht. Dadurch wird Speicherplatz gespart. Aktivieren Sie zur Nutzung dieses Formates das Kontrollkästchen **Thin Provisioning** (für ESX) oder **Laufwerk mit dynamischer Erweiterung** (für Hyper-V).
- **Format 'Thick'.** Das Laufwerk belegt den gesamten bereitgestellten Speicherplatz. Dies verbessert die Performance der virtuellen Maschine. Deaktivieren Sie zur Nutzung des Formates 'Thick' das Kontrollkästchen **Thin Provisioning** (für ESX) oder **Laufwerk mit dynamischer Erweiterung** (für Hyper-V).

Wenn eine physikalische Maschine gesichert wurde, ist die Standardeinstellung das Format 'Thick'. Bei Wiederherstellung des Backups einer virtuellen Maschine versucht die Software, das Laufwerksformat der ursprünglichen Maschine zu reproduzieren. Falls dies nicht möglich ist, wird das Format 'Thick' verwendet.

Die Implementierung von Xen-Maschinen basiert auf Microsoft Virtual PC und hat daher dieselben Einschränkungen: bis zu 3 IDE-Laufwerke und 1 Prozessor. SCSI-Laufwerke werden nicht unterstützt.

Arbeitsspeicher

Anfangseinstellung: Es ist die Standardeinstellung des Virtualisierungsservers, sofern nicht im Backup enthalten.

Dies ist die Menge des Hauptspeichers, der der neuen virtuellen Maschine zugeteilt wird. Der einstellbare Bereich für die Speicherzuteilung hängt von der Hardware des Hosts ab, dessen Betriebssystem und den Einstellungen des Virtualisierungsprodukts. Sie können beispielsweise festlegen, dass die virtuellen Maschinen nicht mehr als 30% des Arbeitsspeichers verwenden dürfen.

Name

Anfangseinstellung: falls nicht im Backup enthalten, **Neue virtuelle Maschine**.

Geben Sie den Namen für die neue virtuelle Maschine ein. Wurde das Backup durch den Agenten für ESX(i) oder den Agenten für Hyper-V erstellt, dann übernimmt die Software den Namen aus der im Backup enthaltenen virtuellen Maschinen-Konfiguration.

Prozessoren

Anfangseinstellung: Es ist die Standardeinstellung des Servers, sofern nicht im Backup enthalten, oder falls die gesicherten Einstellungen vom Virtualisierungsserver nicht unterstützt werden.

Es handelt sich um die Zahl der Prozessoren für die neue virtuelle Maschine. In den meisten Fällen ist sie auf einen Prozessor eingestellt. Wird der Maschine mehr als ein Prozessor zugewiesen, so kann das Ergebnis nicht garantiert werden. Die Zahl virtueller Prozessoren kann durch die CPU-Konfiguration des Hosts, das Virtualisierungsprodukt und das Betriebssystems des Gastes limitiert werden. Üblicherweise stehen mehrere virtuelle Prozessoren auf Hosts zur Verfügung, die selbst mehrere Prozessoren haben. Eine Multi-Core-Host-CPU oder Hyper-Threading kann mehrfache virtuelle Prozessoren auch auf einem Single-Prozessor-Host ermöglichen.

6.3 Wiederherstellung zu einer manuell erstellten virtuellen Maschine

Dieser Abschnitt beschreibt die Konvertierungsmethode (S. 190), bei der Sie selbst eine virtuelle Maschine erstellen und eine Wiederherstellung zu ihr so durchführen, als ob es sich um eine physikalische Maschine handelt.

Um diese Methode verwenden zu können, benötigen Sie eine Lizenz für die Funktionalität 'Acronis Universal Restore (S. 164)'.

6.3.1 Überlegungen vor der Konvertierung

Konvertieren einer UEFI-basierten Maschine

Sollte die ursprüngliche Maschine UEFI (Unified Extensible Firmware Interface) zum Booten verwenden, dann sollten Sie erwägen, eine virtuelle Maschine zu erstellen, die ebenfalls UEFI-basiert ist.

Sollte Ihr Virtualisierungsprodukt kein UEFI unterstützen, dann können Sie eine BIOS-basierte Maschine erstellen, sofern die ursprüngliche Maschine unter Windows lief. Acronis Backup &

Recovery 11.5 passt den Windows-Boot-Modus an die BIOS-Boot-Firmware an und stellt so sicher, dass Windows bootfähig bleibt.

Bei Linux-Betriebssystemen wird eine Änderung des Boot-Modus von UEFI zu BIOS nicht unterstützt. Acronis Backup & Recovery 11.5 kann eine unter Linux laufende, UEFI-basierte Maschine nur dann konvertieren, wenn die Maschine GRUB in Version 1 verwendet und die Zielmaschine ebenfalls UEFI-basiert ist. Weitere Details finden Sie unter 'Unterstützung für UEFI-basierte Maschinen (S. 53)'.

Wahl der Laufwerksschnittstelle

Möglicherweise möchten Sie beim Erstellen der virtuellen Maschine, dass deren Laufwerke eine andere Schnittstelle verwenden als die in der ursprünglichen Maschine.

- Sie möchten beispielsweise alle Laufwerksschnittstellen von IDE zu SCSI ändern, wenn Sie eine Maschine zu ESX(i) migrieren, weil SCSI die Standardlaufwerksschnittstelle bei ESX(i) ist und eine bessere Performance bietet.
- Sie müssen die Laufwerksschnittstelle des Systems von SCSI zu IDE ändern, wenn Sie eine Maschine zu Hyper-V migrieren, weil Hyper-V das Booten von SCSI-Laufwerken nicht unterstützt.

Falls die ursprüngliche Maschine einen selbsterstellten Boot-Loader verwendet, dann stellen Sie das Systemlaufwerk zu einem Laufwerk mit derselben Schnittstelle wieder her – oder konfigurieren Sie den Bootloader manuell. Hintergrund ist, dass bei Änderung der Schnittstelle des Systemlaufwerks sich auch der Name des Boot-Gerätes ändert; der Bootloader verwendet jedoch weiterhin den alten Namen. Eine Konfiguration von GRUB ist normalerweise nicht notwendig, weil Acronis Backup & Recovery 11.5 dies automatisch durchführt.

6.3.2 Auszuführende Schritte

So führen Sie eine Wiederherstellung zu einer manuell erstellten virtuellen Maschine durch

1. [Bei Wiederherstellung von Windows] Bereiten Sie die Windows-Treiber vor (S. 166), die zu der als Ziel dienenden Virtualisierungsplattform passen.

   Bei unter Linux laufenden Maschinen sind die benötigten Treiber normalerweise bereits im Betriebssystem vorhanden.
2. Erstellen Sie ein bootfähiges Medium (S. 285) mit der Universal Restore-Funktionalität, indem Sie den Acronis Bootable Media Builders verwenden.
3. Erstellen Sie eine virtuelle Maschine, indem Sie die systemeigenen Tools Ihres Virtualisierungsproduktes verwenden.
4. Booten Sie die virtuelle Maschine mit dem bootfähigen Medium.
5. [Bei Wiederherstellung von Windows] Sollten Sie dynamische Volumes benötigen, dann erstellen Sie mithilfe der Funktionen zur Laufwerksverwaltung (S. 311) eine Volume-Gruppe.
6. Wählen Sie die Befehle **Aktionen** –> **Recovery**. Bei Konfiguration einer Wiederherstellung:
   - Aktivieren Sie Universal Restore für Linux oder Universal Restore für Windows. Stellen Sie im letzteren Fall die Treiber bereit, die Sie vorbereitet haben.
   - [Bei Wiederherstellung von Windows] Falls Sie logische Volumes benötigen, dann klicken Sie bei Konfiguration der Wiederherstellung auf **RAID/LVM anwenden**. Die LVM-Struktur wird während der Wiederherstellung automatisch neu erstellt (S. 49).
7. Konfigurieren Sie andere Recovery-Einstellungen und führen Sie eine Wiederherstellung genauso wie auf eine physikalische Maschine aus.

7 Speicherung der gesicherten Daten

7.1 Depots

Ein Depot ist ein Ort zum Speichern von Backup-Archiven. Zur leichteren Nutzung und Administration ist ein Depot mit den Metadaten der Archive assoziiert. Auf diese Metadaten Bezug zu nehmen, macht Aktionen mit im Depot gespeicherten Archiven und Backups schneller und bequemer.

Ein Depot kann auf einem lokalen Laufwerk, auf einem Netzlaufwerk, auf einem Wechselmedium oder einem Bandgerät organisiert werden.

Es gibt keine Limits für die Größe eines Depots oder die Zahl der Backups in einem Depot. Sie können die Größe jedes Archivs durch Bereinigung begrenzen. Die Gesamtgröße aller Archive, die in einem Depot gespeichert werden können, wird jedoch nur von dessen Speichergröße begrenzt.

Warum sollten Sie ein Depot erstellen?

Es wird empfohlen, dass Sie ein Depot an jedem Zielort erstellen, wo Sie Backup-Archive speichern werden. Das erleichtert Ihre Arbeit auf folgende Weise.

Schneller Zugriff auf ein Depot

Sie müssen sich niemals Pfade zu Ordnern merken, in denen die Archive gespeichert werden. Beim Erstellen eines Backup-Plans oder eines Tasks, der die Wahl eines Archivs bzw. eines Archiv-Zielortes benötigt, ist die Depot-Liste zum schnellen Zugriff verfügbar, damit Sie den Verzeichnisbaum nicht durchsuchen müssen.

Leichte Verwaltung der Archive

Sie können auf ein Depot aus dem Fensterbereich **Navigation** zugreifen. Wenn Sie ein Depot ausgewählt haben, können Sie die dort gespeicherten Archive durchsuchen und mit ihnen folgende Verwaltungsaktionen durchführen:

- Eine Liste der in jedem Archiv enthaltenen Backups abfragen
- Daten aus einem Backup wiederherstellen
- Den Inhalt eines Backups untersuchen
- Alle oder bestimmte Archive bzw. Backups in dem Depot validieren
- Ein Volume-Backup mounten, um Dateien aus dem Backup auf ein physikalisches Laufwerk zu kopieren
- Archive bzw. Backups aus Archiven sicher löschen.

Die Erstellung von Depots ist zwar sehr empfehlenswert, aber nicht obligatorisch. Sie können auf die Verwendung von Verknüpfungen verzichten und stattdessen immer den Pfad zum Speicherort angeben.

Die Erstellung eines Depots führt schließlich dazu, dass sein Name zum Abschnitt **Depots** im Fensterbereich **Navigation** hinzugefügt wird.

Zentrale und persönliche Depots

Ein zentrales Depot ist ein im Netzwerk liegender Speicherort, der vom Administrator des Management Servers zugeteilt wird, um als Speicherplatz für die Backup-Archive zu dienen. Ein

zentrales Depot kann von einem Storage Node verwaltet werden (verwaltetes Depot) oder es wird nicht verwaltet. Weitere Informationen finden Sie im Abschnitt 'Zentrale Depots (S. 203)'.

Ein Depot wird als persönlich bezeichnet, wenn es durch direkte Verbindung der Konsole zu einer verwalteten Maschine erstellt wurde. Persönliche Depots sind spezifisch für jede verwaltete Maschine.

Ansicht 'Depots'

Depots (im Fensterbereich 'Navigation') – oberstes Element des Verzeichnisbaums 'Depots'. Klicken Sie auf dieses Element, um die zentralen und persönlichen Depots angezeigt zu bekommen. Verwenden Sie die im oberen Bereich der Ansicht **Depots** liegende Symbolleiste, um Aktionen auf ein Depot anzuwenden. Zu zentralen Depots siehe den Abschnitt 'Aktionen für zentrale Depots (S. 204)'. Zu persönlichen Depots siehe den Abschnitt 'Aktionen für persönliche Depots (S. 214)'.

- **Zentrale Depots.** Diese Depots sind verfügbar, wenn die Konsole mit einer verwalteten Maschine oder mit dem Management Server verbunden ist.
- **Persönliche Depots.** Diese Depots sind verfügbar, wenn die Konsole mit einer verwalteten Maschine verbunden ist.

Klicken Sie auf ein Depot im Depot-Verzeichnisbaum, um eine Detailansicht dieses Depots (S. 202) zu öffnen und führen Sie dann Aktionen mit den dort gespeicherten Archiven (S. 280) und Backups (S. 280) aus.

7.1.1 Mit Depots arbeiten

Dieser Abschnitt beschreibt kurz die Hauptelemente der Benutzeroberfläche für ein ausgewähltes Depot und macht Vorschläge, wie Sie damit arbeiten können.

Informationen über ein Depot ermitteln

Die Informationen über ein bestimmtes Depot befinden sich im oberen Fensterbereich eines angewählten Depots. Durch Verwendung der gestapelten Symbolleiste können Sie die Auslastung des Depots abschätzen. Die Auslastung des Depots entspricht dem Verhältnis von freiem und belegtem Speicherplatz im Depot (nicht verfügbar, falls sich das Depot auf einer Bandbibliothek befindet). Der freie Speicherplatz entspricht dem Speicherplatz des Speichergeräts, auf dem sich das Depot befindet. Wenn das Depot beispielsweise auf einem Festplattenlaufwerk liegt, dann entspricht der freie Speicherplatz des Depots dem freien Platz dieses entsprechenden Volumes. Der belegter Speicherplatz entspricht der Gesamtgröße aller Backup-Archive und ihrer Metadaten, sofern in dem Depot vorliegend.

Sie können außerdem die Gesamtzahl aller in diesem Depot gespeicherter Archive und Backups erhalten – sowie den vollständigen Pfad zum Depot.

Nur bei verwalteten Depots können Sie den Namen des Storage Nodes ermitteln, der das Depot verwaltet – sowie die Stadien zur Verschlüsselung und Deduplizierung (S. 259).

Durchsuchen des Depot-Inhalts und Datenauswahl

Sie können zum Durchsuchen des Depot-Inhalts sowie zur Auswahl von Daten für eine Wiederherstellung die Registerlaschen **Datenanzeige** oder **Archiv-Anzeige** verwenden.

Datenanzeige

Die Registerlasche **Datenanzeige** ermöglicht Ihnen, die Backup-Daten nach Versionen zu durchsuchen und auszuwählen (nach Datum und Zeitpunkt der Backup-Erstellung). Die

Registerlasche **Datenanzeige** teilt sich die Funktionalität zur Suche und Katalogisierung mit dem Datenkatalog (S. 150).

Archiv-Anzeige

In der Registerlasche **Archiv-Anzeige** werden die gesicherten Daten nach Archiven angezeigt. Verwenden Sie die **Archiv-Anzeige**, um Aktionen mit im Depot gespeicherten Archiven und Backups durchzuführen. Zu weiteren Informationen über diese Aktionen siehe folgende Abschnitte:

- 'Aktionen mit im Depot gespeicherten Archiven (S. 280)'.
- 'Aktionen mit Backups (S. 280)'.
- 'Tabellenelemente sortieren, filtern und konfigurieren (S. 29)'.

Welche Bedeutung hat das Symbol ?

Beim Durchsuchen von Archiven in der Registerkarte **Archiv-Anzeige** fällt Ihnen möglicherweise ein Backup mit dem Symbol auf. Dieses Symbol bedeutet, dass das Backup zum Löschen gekennzeichnet ist, aber aus einem der nachfolgenden Gründe nicht sofort gelöscht werden kann.

- Andere Backups hängen von diesem ab; eine Konsolidierung ist jedoch nicht möglich oder wurde durch die Aufbewahrungsregeln deaktiviert.
- Das Backup ist auf einem Band gespeichert.

Sie können keine Aktionen mit solchen Backups durchführen, die zum Löschen gekennzeichnet sind. Sie verschwinden aus der **Archiv-Anzeige**, nachdem Sie physikalisch gelöscht wurden. Dazu kommt es, wenn auch alle abhängigen Backups gelöscht wurden, das Band überschrieben wurde oder nach der nächsten Bereinigung, nachdem Sie in den Aufbewahrungsregeln die Konsolidierung aktiviert haben.

7.1.2 Zentrale Depots

Ein zentrales Depot ist ein im Netzwerk liegender Speicherort, der vom Administrator des Management Servers zugeteilt wird, um als Speicherplatz für die Backup-Archive zu dienen. Ein zentrales Depot kann von einem Storage Node **verwaltet** werden oder es ist **nicht verwaltet**. Die Zahl und die Größe der Archive, die in einem zentralen Depot gespeichert werden können, werden nur von der Speichergröße begrenzt.

Sobald der Administrator ein zentrales Depot erstellt, werden dessen Name und der Pfad zum Depot an alle auf dem Server registrierten Maschinen verteilt. Die Verknüpfung zum Depot erscheint auf den Maschinen in der Gruppe **Depots**. Jeder Backup-Plan, der auf den Maschinen existiert, einschließlich lokaler Pläne, kann das zentrale Depot benutzen.

Die folgende Tabelle erläutert den Unterschied zwischen verwalteten und nicht verwalteten Depots im Detail.

Funktionalität	Verwaltete Depots	Nicht verwaltete Depots
Erfordert die Installation des Acronis Backup & Recovery 11.5 Storage Nodes	Ja	Nein
Im Depot gespeicherte Daten sind im zentralen Datenkatalog (S. 150) enthalten	Ja	Nein

Dedizierte Benutzerkonten, um auf ein Depot zuzugreifen (Depot-Administratoren (S. 209) und Depot-Benutzer (S. 210))	Ja	Nein
Datendeduplizierung (S. 259)	Ja	Nein
Verschlüsselung des Depots (S. 208)	Ja	Nein
Archiv-Bereinigung, Replikation und Validierung per Backup-Plan werden durchgeführt von...	...dem Storage Node (S. 247) (Replikationen zum Online Backup Storage ausgenommen, werden vom Agenten durchgeführt).	...dem Agenten.
Unterstützte Storage-Typen:		
Acronis Online Backup Storage	Nein	Ja
Bandgerät	Ja (keine Deduplizierung oder Depot-Verschlüsselung)	Nein
Freigegebenes Netzlaufwerk	Ja	Ja
SAN, NAS	Ja	Ja
FTP/SFTP-Server	Nein	Ja

7.1.2.1 Aktionen für zentrale Depots

Zugriff auf Aktionen

1. Verbinden Sie die Konsole mit dem Management Server.
2. Klicken Sie im Fensterbereich **Navigation** auf **Depots** –> **Zentral**.

Alle hier beschriebenen Aktionen werden durch Klicken auf die korrespondierenden Schaltflächen in der Depot-Symbolleiste ausgeführt. Sie können auf diese Aktionen auch über das Hauptmenüelement **[Depot-Name] Aktionen** zugreifen.

Nachfolgend finden Sie eine Anleitung zur Durchführung von Aktionen mit zentralen Depots.

Aufgabe	Lösung
Ein verwaltetes oder nicht verwaltetes Depot erstellen	1. Klicken Sie auf **Erstellen**. 2. Bestimmen Sie im Feld **Typ** die gewünschte Variante des Depots: **Verwaltet** oder **Nicht verwaltet**. Die Prozedur zur Erstellung zentraler Depots wird ausführlich in den nachfolgenden Abschnitten beschrieben: ▪ Ein zentrales, verwaltetes Depot erstellen (S. 206) ▪ ein zentrales, nicht verwaltetes Depot erstellen (S. 210)
Ein verwaltetes oder nicht verwaltetes Depot bearbeiten	1. Wählen Sie das Depot. 2. Klicken Sie auf **Bearbeiten**. Abhängig vom gewählten Depot (verwaltet oder nicht verwaltet) öffnet sich eine entsprechende Seite zur Bearbeitung: ▪ Auf der Seite **Verwaltetes Depot bearbeiten** können Sie den Depot-Namen, Benutzerkonten sowie die Informationen im Feld **Kommentare** ändern. ▪ Auf der Seite **Nicht verwaltetes Depot bearbeiten** können Sie den Depotnamen sowie die Informationen im Feld **Kommentare** bearbeiten.

Aufgabe	Lösung
Ein verwaltetes Depot trennen	1. Wählen Sie das Depot. 2. Klicken Sie auf **Trennen**. Durch das Trennen eines Depots wird auch die Zuordnung zwischen dem Depot und dem Storage Node entfernt und dieses Depot aus der Benutzeroberfläche gelöscht. Nichtsdestotrotz verbleiben alle im Depot gespeicherten Archive davon unberührt. Pläne und Tasks, die dieses Depot verwenden, werden als Resultat der Aktion fehlschlagen. Sie können dieses getrennte Depot aber später immer noch wieder an denselben oder einen anderen Storage Node anbinden. **Anmerkungen** ■ Bandbasierte Depots können nicht getrennt werden. ■ Um ein Depot von einem nicht verfügbaren Storage Node zu trennen, entfernen Sie den Storage Node (S. 250) vom Management Server.
Das zuvor getrennte, verwaltete Depot anschließen	Klicken Sie auf **Anschließen**. Die Prozedur zum Anschließen eines verwalteten Depots an einen Storage Node wird ausführlich im Abschnitt Ein verwaltetes Depot anschließen (S. 211) beschrieben. **Hinweis**. Bandbasierte Depots können nicht angeschlossen werden.
Ein Depot validieren	1. Wählen Sie das Depot. 2. Klicken Sie auf **Validieren**. Sie gelangen zur Seite Validierung (S. 266) mit dem bereits als Quelle vorausgewählten Depot. Die Validierung des Depots überprüft alle in diesem Depot enthaltenen Archive.
Einen nicht verwalteten Depot-Ordner öffnen	1. Wählen Sie das nicht verwaltete Depot. 2. Klicken Sie auf **Durchsuchen**. Das Depot ist danach zur Untersuchung mit dem Standard-Datei-Manager verfügbar.
Ein Depot löschen	1. Wählen Sie das Depot. 2. Klicken Sie auf **Löschen**. Das Depot wird zusammen mit allen in diesem gespeicherten Archiven gelöscht. Pläne und Tasks, die dieses Depot verwenden, werden als Resultat der Aktion fehlschlagen.
Benutzer-Anmeldedaten für den Zugriff auf ein Depot ändern.	Klicken Sie auf **Benutzer ändern**. Eine Änderung der Anmeldedaten ist nur für solche Depots verfügbar, die auf einem gemeinsam benutzten Speicherort liegen.
Informationen eines Depots aktualisieren	Klicken Sie auf **Aktualisieren**. Während Sie den Inhalt eines Depots einsehen, können Archive dem Depot hinzugefügt, aus diesem gelöscht oder modifiziert werden. Klicken Sie auf **Aktualisieren**, damit die neuesten Veränderungen für die Depot-Informationen berücksichtigt werden.

Ein zentrales, verwaltetes Depot erstellen

So erstellen Sie ein zentrales, verwaltetes Depot

Depot

Name

Geben Sie dem Depot einen eindeutigen Namen. Eine Erstellung von zwei zentralen Depots mit gleichem Namen ist nicht gestattet.

Kommentare

[Optional] Vergeben Sie für das zu erstellende Depot eine charakteristische Beschreibung.

Typ

Wählen Sie den Typ **Verwaltet**.

Storage Node

Bestimmen Sie den Acronis Backup & Recovery 11.5 Storage Node, der das Depot verwalten wird.

Deduplizierung

[Optional] Bestimmen Sie, ob eine Archiv-Deduplizierung für das Depot aktiviert werden soll. Eine Deduplizierung reduziert den von Archiven belegten Speicherplatz und die Datenübertragungsmenge für Backups. Sie reduziert die Größe der im Depot liegenden Archive, indem redundante Daten (wie doppelte Dateien und Festplatten-Datenblöcke) eliminiert werden.

Auf Bandgeräten ist keine Deduplizierung möglich.

Deduplizierung ist nicht möglich, falls der Storage Node unter einem 32-Bit-Betriebssystem installiert ist.

Um mehr darüber zu erfahren, wie Deduplizierung funktioniert, siehe den Abschnitt Deduplizierung (S. 259).

Verschlüsselung (S. 208)

[Optional] Bestimmen Sie, ob das Depot per Verschlüsselung geschützt werden soll. Alle zum Depot geschriebenen Daten werden verschlüsselt und alle von ihm gelesenen werden durch den Storage Node wieder transparent entschlüsselt (unter Verwendung eines Depot-spezifischen, auf dem Storage Node hinterlegten Kodierungsschlüssels).

Ein auf einem Bandgerät befindliches Depot kann nicht per Verschlüsselung geschützt werden.

Pfad (S. 208)

Spezifizieren Sie, wo das Depot erstellt wird. Verwaltete Depots können auf einer Netzwerkfreigabe, einem SAN, NAS, Bandgerät oder auf einer für den Storage Node lokalen Festplatte liegen.

Deduplizierungsdatenbank zusammen mit den Backups unterbringen (nur verfügbar, wenn die Funktion **Deduplizierung** aktiviert ist)

Die Deduplizierungsdatenbank sichert die Hash-Werte aller im Depot gespeicherten Elemente – mit Ausnahme solcher, die nicht dedupliziert werden können (wie etwa verschlüsselte Dateien).

Das Depot wird auf einem für den Storage Node lokalen Laufwerk erstellt, die Deduplizierungsdatenbank wird im selben Depot platziert (das Kontrollkästchen **Deduplizierungsdatenbank zusammen mit Backups unterbringen** ist aktiviert).

Falls das Depot auf einer Netzwerkfreigabe erstellt wird, ist das Kontrollkästchen **Deduplizierungsdatenbank zusammen mit Backups unterbringen** deaktiviert – folglich müssen Sie den Pfad zur Deduplizierungsdatenbank manuell spezifizieren.

Die gemeinsame Speicherung von Deduplizierungsdatenbank und Backups kann zu einer gewissen Herabsetzung der System-Performance führen. Zur Verbesserung der System-Performance empfehlen wir, die Deduplizierungsdatenbank und das verwaltete Depot auf unterschiedlichen Laufwerken zu erstellen.

Deduplizierungsdatenbank (S. 208) (nur verfügbar, falls die **Deduplizierung** aktiviert ist).

Spezifizieren Sie einen Ordner auf den lokalen Laufwerken des Storage Nodes oder SAN, um dort die Deduplizierungsdatenbank zu erstellen.

Laufwerke

[Optional] Falls das Depot auf einem Bandgerät erstellt wird, dann spezifizieren Sie auch das/die Bandgerät(e), welche(s) bei Backups zu dem Depot verwendet werden soll. Standardmäßig werden alle verfügbaren Laufwerke verwendet. Klicken Sie auf den nach unten zeigenden Pfeil und (de)aktivieren Sie die erforderlichen Kontrollkästchen.

Band-Pool:

[Optional] Falls das Depot auf einem Bandgerät erstellt wird, dann spezifizieren Sie auch den Pool, dessen Bänder vom Depot verwendet werden sollen. Standardmäßig ist der Pool **Acronis** vorausgewählt.

Katalogdatenbank

[Optional] Spezifizieren Sie, wo die Datenbank des Datenkatalogs gespeichert werden soll.

Abwärtskompatibilität

Klicken Sie auf **Abwärtskompatibilität anzeigen**, um auf diese Option zugreifen zu können.

[Optional] Wählen Sie, ob das Depot abwärtskompatibel mit den Acronis Backup & Recovery 10 Agenten gemacht werden soll.

Was Sie über abwärtskompatible Depots wissen müssen:

- Ein auf einem Bandgerät befindliches Depot kann nicht abwärtskompatibel sein.

– Die Agenten von Acronis Backup & Recovery 11 und Acronis Backup & Recovery 11.5 können Backups zu einem Depot durchführen, unabhängig von dessen Abwärtskompatibilitätseigenschaft.

– Sie können für ein abwärtskompatibles Depot keine Depot-Administratoren und Depot-Benutzer spezifizieren.

- Wenn die Konsole mit einem Acronis Backup & Recovery 10 Agenten verbunden ist, dann wird die Registerkarte **Datenanzeige** für ein Depot nicht angezeigt.

- Backups, die von Acronis Backup & Recovery 11 und Acronis Backup & Recovery 11.5 erstellt wurden, werden automatisch katalogisiert. Um auch Backups, die von Acronis Backup & Recovery 10 erstellt wurden, in den Datenkatalog aufzunehmen, klicken Sie in der Registerkarte **Datenanzeige** des Depots auf den Link **Katalog jetzt aktualisieren**. Beachten Sie, dass die Katalogisierung eine zeit- und ressourcenintensive Prozedur ist.

Komprimierung

[Optional] Bestimmen Sie, ob die Deduplizierungsdatenspeicher komprimiert werden sollen. Diese Einstellung ist nur verfügbar, falls die Abwärtskompatibilität eingeschaltet und die Deduplizierungsfunktion aktiviert ist.

Benutzerkonten

Depot-Administratoren (S. 209)

Fügen Sie Gruppen oder Benutzerkonten hinzu, die Administratorrechte auf diesem Depot haben sollen. Depot-Administratoren können alle im Depot gespeicherten Archive einsehen und verwalten. Zudem werden alle Acronis Centralized Admins und Mitglieder der Gruppe 'Administratoren' des Storage Nodes standardmäßig als Depot-Administratoren betrachtet.

Depot-Benutzer (S. 210)

Fügen Sie Gruppen oder Benutzerkonten hinzu, die Benutzerrechte auf diesem Depot haben sollen. Depot-Benutzer können nur ihre eigenen, im Depot gespeicherten Archive einsehen und verwalten. Standardmäßig wird die Gruppe 'Jeder' des Storage Nodes den Depot-Benutzern hinzugefügt.

Nachdem Sie alle notwendigen Schritte durchgeführt haben, klicken Sie auf **OK**, um die Erstellung des verwalteten Depots auszuführen.

Pfad zum Depot

So spezifizieren Sie den Pfad, wo das verwaltete Depot erstellt wird

1. Tragen Sie den vollständigen Pfad zum Verzeichnis in das Feld **Pfad** ein oder wählen Sie den gewünschten Ordner im Verzeichnisbaum. Verwaltete Depots können organisiert werden:
   - Auf für den Storage Node lokal verfügbaren Festplatten.
   - Auf einer Netzwerkfreigabe.
   - Auf einem Storage Area Network (SAN).
   - Auf einem Network Attached Storage-Gerät (NAS).
   - Auf einer Bandbibliothek, die lokal mit dem Storage Node verbunden ist.

   Um am gewählten Speicherort für das Depot einen neuen Ordner zu erstellen, klicken Sie auf  **Ordner erstellen**.
2. Klicken Sie auf **OK**.

Ein Depot kann nur in einem leeren Ordner angelegt werden.

Es wird nicht empfohlen, ein selbst deduplizierendes *verwaltetes Depot auf einem FAT32-Volume zu erstellen. Ein solches Depot könnte alle deduplizierten Elemente möglicherweise in zu große Dateien speichern. Weil die maximale Dateigröße in den FAT-Dateisystemen auf 4 GB begrenzt ist, könnte der Storage Node aufhören zu arbeiten, wenn diese Grenze erreicht ist.*

Pfad zur Deduplizierungsdatenbank

So spezifizieren Sie den Pfad, wo die Deduplizierungsdatenbank erstellt wird

1. Wählen Sie aus den **Lokalen Ordnern** des Storage Nodes das gewünschte Verzeichnis aus oder geben Sie seinen vollständigen Pfad in das Feld **Pfad** ein.

   Um für die Datenbank einen neuen Ordner zu erstellen, klicken Sie auf **Ordner erstellen**.

   Wir empfehlen dringend, dass Sie den Empfehlungen folgen, die im Bereich 'Ein Laufwerk für eine Deduplizierungsdatenbank wählen' des Abschnitts 'Optimale Vorgehensweisen bei der Deduplizierung (S. 263)' gegeben werden.
2. Klicken Sie auf **OK**.

Verschlüsselung des Depots

Wenn Sie ein Depot durch Verschlüsselung schützen, werden alle zu diesem Depot geschriebenen Daten verschlüsselt und alle von ihm gelesenen durch den Storage Node wieder transparent entschlüsselt (unter Verwendung eines Depot-spezifischen, auf dem Storage Node hinterlegten Kodierungsschlüssels). Falls das Speichermedium gestohlen wird oder eine unbefugte Person darauf

zugreift, wird der Übeltäter den Inhalt des Depots ohne Zugriff auf den Storage Node nicht entschlüsseln können.

Diese Verschlüsselung hat nichts mit der Verschlüsselung von Archiven zu tun, wie sie über einen Backup-Plan spezifiziert und durch einen Agenten ausgeführt wird. Sollte ein Archiv bereits verschlüsselt sein, dann wird die Verschlüsselung aufseiten des Storage Nodes noch einmal über die durch den Agenten ausgeführte gelegt.

So schützen Sie ein Depot per Verschlüsselung

1. Wählen Sie einen der folgenden Verschlüsselungsalgorithmen aus der Dropdown-Liste:
   - **AES 128** – die Depot-Inhalte werden mit dem Advanced Encryption Standard-Verfahren (AES) und einer Tiefe von 128-Bit verschlüsselt.
   - **AES 192** – der Depot-Inhalt wird mit dem Advanced Standard Encryption-Verfahren (AES) und einer Tiefe von 192-Bit verschlüsselt.
   - **AES 256** – der Depot-Inhalt wird mit dem Advanced Standard Encryption-Verfahren (AES) und einer Tiefe von 256-Bit verschlüsselt.
2. Spezifizieren Sie im Feld **Kennwort eingeben** ein Wort, welches zum Erzeugen des Kodierungsschlüssels verwendet wird.

   Details: Das Kennwort unterscheidet Groß-/Kleinschreibung. Das Kennwort wird nur bei Anschluss des Depots an einen anderen Storage Node abgefragt.
3. Geben Sie im Feld **Bestätigen** das eben eingegebene Kennwort erneut ein.
4. Klicken Sie auf **OK**.

Der kryptografische AES-Algorithmus arbeitet im 'Cipher Block Chaining Mode' (CBC) und verwendet einen zufällig erstellten Schlüssel mit einer benutzerdefinierten Größe von 128, 192 oder 256 Bit. Je größer die Schlüsselgröße, desto länger wird das Programm für die Verschlüsselung der im Depot gespeicherten Archive benötigen, aber desto sicherer sind auch die Daten.

Der Kodierungsschlüssel ist dann mit AES-256 verschlüsselt, wobei ein SHA-256-Hash-Wert des gewählten Kennworts als Schlüssel dient. Das Kennwort selbst wird nirgendwo auf dem Laufwerk gespeichert, es wird nur der Kennwort-Hash-Wert für Bestätigungszwecke verwendet. Mit dieser zweistufigen Methode sind die Archive vor jedem unberechtigten Zugriff geschützt, aber ein verlorenes Kennwort kann unmöglich wiederhergestellt werden.

Depot-Administratoren

Depot-Administratoren können Backups zu diesem Depot erstellen sowie jedes auf dem Depot gespeicherte Archiv einsehen und verwalten. Standardmäßig wird die Gruppe 'Administratoren' des Storage Nodes den 'Depot-Administratoren' hinzugefügt.

So fügen Sie eine Gruppe oder Benutzerkonten hinzu

1. Geben Sie die Namen der Gruppen oder Benutzer in die jeweiligen Felder nach folgenden Mustern ein:
   - *Anzeigename* (Beispiel: **Vorname Nachname**).
   - *Benutzername* (Beispiel: **Benutzer1**).
   - *Objektname@Domainname* (Beispiel: **Benutzer1@Domain1**).
   - *Domainname\Objektname* (Beispiel: **Domain1\Benutzer1**).
2. Klicken Sie auf **Namen überprüfen**, sobald Sie diese eingegeben haben. Klicken Sie auf **OK**, wenn der Namen gefunden wurde (die Schaltfläche **OK** ist solange deaktiviert, bis der Name gefunden wurde).

Löschen Sie den Namen und geben Sie einen neuen ein, wenn kein entsprechendes Objekt gefunden wurde. Sollten mehrere Objekte für den eingegebenen Namen gefunden werden, dann wählen Sie eines davon aus und klicken anschließend auf **OK** – oder Sie klicken auf **Abbrechen** und spezifizieren einen anderen Namen.

Die Software versucht zuerst, die eingegebenen Namen in der Liste der lokalen Benutzer und Gruppen auf der Maschine zu finden, auf der der Storage Node installiert ist. Wurde nichts gefunden, dann überprüft die Software die Domain-Benutzer und Gruppen.

Sie werden aufgefordert, die Anmeldedaten des Domain-Kontos zu spezifizieren, wenn Sie einen Benutzer- oder Gruppennamen eingeben, der nicht durch Verwendung Ihres Domain-Kontos überprüft werden kann. Beispielsweise, wenn Sie mit einem anderen Domain-Konto angemeldet sind als dem von Ihnen zur Überprüfung angegebenen Domain-Namen.

Depot-Benutzer

Depot-Benutzer können nur ihre eigenen, im Depot gespeicherten Archive einsehen und verwalten. Ein Depot-Benutzer, der auf einer Maschine Mitglied der Gruppe 'Administratoren' ist, kann zusätzlich jedes Archiv einsehen und verwalten, das von dieser Maschine in einem verwalteten Depot erstellt wurde. Standardmäßig wird die Gruppe 'Jeder' des Storage Nodes den 'Depot-Benutzern' hinzugefügt.

So fügen Sie eine Gruppe oder Benutzerkonten hinzu

1. Geben Sie die Namen der Gruppen oder Benutzer in die jeweiligen Felder nach folgenden Mustern ein:
   - *Anzeigename* (Beispiel: **Vorname Nachname**).
   - *Benutzername* (Beispiel: **Benutzer1**).
   - *Objektname@Domainname* (Beispiel: **Benutzer1@Domain1**).
   - *Domainname\Objektname* (Beispiel: **Domain1\Benutzer1**).
2. Klicken Sie auf **Namen überprüfen**, sobald Sie diese eingegeben haben. Klicken Sie auf **OK**, wenn der Namen gefunden wurde (die Schaltfläche **OK** ist solange deaktiviert, bis der Name gefunden wurde).

   Löschen Sie den Namen und geben Sie einen neuen ein, wenn kein entsprechendes Objekt gefunden wurde. Sollten mehrere Objekte für den eingegebenen Namen gefunden werden, dann wählen Sie eines davon aus und klicken anschließend auf **OK** – oder Sie klicken auf **Abbrechen** und spezifizieren einen anderen Namen.

   Die Software versucht zuerst, die eingegebenen Namen in der Liste der lokalen Benutzer und Gruppen auf der Maschine zu finden, auf der der Storage Node installiert ist. Wurde nichts gefunden, dann überprüft die Software die Domain-Benutzer und Gruppen.

   Sie werden aufgefordert, die Anmeldedaten des Domain-Kontos zu spezifizieren, wenn Sie einen Benutzer- oder Gruppennamen eingeben, der nicht durch Verwendung Ihres Domain-Kontos überprüft werden kann. Beispielsweise, wenn Sie mit einem anderen Domain-Konto angemeldet sind als dem von Ihnen zur Überprüfung angegebenen Domain-Namen.

Ein zentrales, nicht verwaltetes Depot erstellen

Anders als bei zentral verwalteten Depots werden die Daten von unverwalteten Depots nicht in den zentralen Datenkatalog (S. 150) aufgenommen. Sie können jedoch bei jedem Depot die Registerkarte **Datenanzeige** verwenden, um dessen Daten zu durchsuchen.

So erstellen Sie ein zentrales, nicht verwaltetes Depot

Depot

Name

Geben Sie dem Depot einen eindeutigen Namen. Eine Erstellung von zwei zentralen Depots mit gleichem Namen wird nicht gestattet.

Kommentare

Vergeben Sie für das zu erstellende Depot eine charakteristische Beschreibung.

Typ

Wählen Sie den Typ **Nicht verwaltet**.

Pfad (S. 211)

Spezifizieren Sie, wo das Depot erstellt wird.

Nachdem Sie alle notwendigen Schritte durchgeführt haben, klicken Sie auf **OK**, um die Erstellung des nicht verwalteten, zentralen Depots auszuführen.

Pfad zum Depot

So spezifizieren Sie den Pfad, wo das nicht verwaltete Depot erstellt wird

1. Geben Sie den vollständigen Pfad zum Verzeichnis in das Feld 'Pfad' ein, oder wählen Sie den gewünschten Ordner aus dem Verzeichnisbaum. Nicht verwaltete Depots können organisiert werden:
   - Acronis Online Backup Storage
   - auf einer Netzwerkfreigabe
   - auf einem Storage Area Network (SAN)
   - auf einem Network Attached Storage-Gerät (NAS)
   - auf FTP- und SFTP-Servern.

   Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

   Um für das Depot einen neuen Ordner zu erstellen, klicken Sie auf  'Ordner erstellen'.

   Ein Depot kann nur in einem leeren Ordner angelegt werden.

2. Klicken Sie auf OK.

Ein verwaltetes Depot anschließen

Ein Depot, das von einem Storage Node verwaltet wird, kann von diesem getrennt (S. 204) und an einen anderen angeschlossen werden. Als Folge stoppt der alte Storage Node die Verwaltung des Depots, während der neue mit der Verwaltung des Depots beginnt. Das kann notwendig werden, wenn Sie Storage Node-Hardware ausrangieren, der Storage Node verloren ging oder Sie einen Storage Node neu installieren.

Falls der alte Storage Node nicht mehr verfügbar ist, dann entfernen Sie diesen (S. 250) vom Management Server, bevor Sie die Depots des alten an einen neuen Storage Node anschließen.

Hinweis: *Persönliche, zentrale nicht verwaltete und bandbasierte Depots können nicht angeschlossen werden.*

Vor dem Anschluss einer

Katalogdatenbank

Empfehlen wir, dass Sie die Katalogdatenbank des Depots vom alten Storage Node zu dem neuen verschieben. Anderenfalls müssen Sie das Depot erneut katalogisieren, was eine längere Zeit dauern kann.

Die Depot-Katalogdatenbank ist eine Zusammenstellung von Dateien, die sich in einem Ordner befinden, dessen Namen der GUID des Depots entspricht. Ändern Sie den Ordnernamen nicht, wenn Sie ihn verschieben. Um die GUID eine korrekt angeschlossenen Depots zu ermitteln, suchen Sie im Depot-Ordner nach einer Datei mit dem Namen <Depot-GUID>**_L.FDB**.

Der Standardspeicherort der Katalogdatenbanken auf einem Storage Node ist wie folgt:

- In Windows XP und Server 2003: **%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\ASN\Catalog**.
- In Windows Vista und späteren Versionen von Windows: **%PROGRAMDATA%\Acronis\BackupAndRecovery\ASN\Catalog**.

Deduplizierungsdatenbank

Bei einem deduplizierenden Depot empfehlen wir, dass Sie die Deduplizierungsdatenbank von dem alten zum neuen Storage Node verschieben. Anderenfalls wird die Software die Deduplizierungsdatenbank automatisch neu erstellen, was eine längere Zeit dauern kann.

Weitere Informationen über den empfohlenen Speicherort für die Deduplizierungsdatenbank finden Sie im Abschnitt 'Optimale Vorgehensweisen bei der Deduplizierung (S. 263)'.

Die Deduplizierungsdatenbank besteht aus mehreren Dateien mit der Bezeichnung <Depot-GUID>**_u.***. Um die GUID eine korrekt angeschlossenen Depots zu ermitteln, suchen Sie im Depot-Ordner nach einer Datei mit dem Namen <Depot-GUID>**_L.FDB**.

Depot-Datenbank

Die Depot-Datenbank enthält die Metadaten aller im Depot gespeicherter Archive. Normalerweise wird bei Trennung eines Depots vom Storage Node die Depot-Datenbank von ihrem Standardspeicherort zu dem Depot verschoben, das gerade getrennt wird. Die Software sucht beim Anschließen des Depots nach der Datenbank im Depot. Falls die Depot-Datenbank gefunden wurde, wird diese zu dem Standardspeicherort auf demjenigen Storage Node verschoben, an den das Depot angeschlossen wird. Falls die Datenbank nicht im Depot gefunden wird, werden Sie aufgefordert, den Pfad zu dieser Datenbank manuell zu spezifizieren.

Der Standardspeicherort einer Depot-Datenbank auf einem Storage Node ist wie folgt:

- In Windows XP und Server 2003: **%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\ASN\VaultMetadataDatabases**.
- In Windows Vista und späteren Versionen von Windows: **%PROGRAMDATA%\Acronis\BackupAndRecovery\ASN\VaultMetadataDatabases**.

So schließen Sie ein verwaltetes Depot an einen Storage Node an

Depot

Storage Node

Wählen Sie den Storage Node, der das Depot verwalten soll.

Pfad

Spezifizieren Sie den Pfad zu dem getrennten Depot.

Depot-Datenbank

Spezifizieren Sie, wo sich die Depot-Datenbank befindet. Dieser Abschnitt erscheint nur, wenn der Storage Node die Datenbank innerhalb des Depots nicht finden kann.

Falls die Datenbank in dem von Ihnen spezifizierten Ordner gefunden wurde, wird sie zu dem Standardspeicherort auf demjenigen Storage Node verschoben, an den das Depot angeschlossen wird. Anderenfalls wird der Storage Node die Metadaten abrufen und die Datenbank in dem zuvor erwähnten Standardspeicherort neu erstellen.

Deduplizierungsdatenbank

Spezifizieren Sie den Ordner, in dem sich die Deduplizierungsdatenbank des Depots befindet. Sollte die Datenbank in dem von Ihnen spezifizierten Ordner nicht gefunden werden, dann wird sie dort neu erstellt.

Der Datenbankpfad wird automatisch eingegeben, falls die Datenbank im Depot-Ordner gespeichert ist.

Katalogdatenbank

Spezifizieren Sie den Ordner, wo sich die Katalogdatenbank des Depots befindet. (Lautet der Pfad der Depot-Katalogdatenbank beispielsweise **E:\Katalog_db\AAAAAAAA-BBBB-CCCC-DDDD-EEEEEEEEEEEE**, dann spezifizieren Sie **E:\Katalog_db**.) Wird die Katalogdatenbank in dem von Ihnen spezifizierten Ordner nicht gefunden, dann wird das angeschlossene Depot als nicht katalogisiert angesehen.

Kennwort

Stellen Sie für ein verschlüsseltes Depot das entsprechende Kennwort zur Verfügung.

Nachdem Sie alle notwendigen Schritte durchgeführt haben, klicken Sie auf **OK**, um das Anschließen des Depots auszuführen.

7.1.3 Persönliche Depots

Ein Depot wird als persönlich bezeichnet, wenn es durch direkte Verbindung der Konsole zu einer verwalteten Maschine erstellt wurde. Persönliche Depots sind spezifisch für jede verwaltete Maschine. Persönliche Depots sind für jeden Benutzer sichtbar, der sich am System anmelden kann. Die Berechtigungen eines Benutzers, Backups zu einem persönlichen Depot durchzuführen, werden über die Zugriffsrechte definiert, die dieser Benutzer für den Ordner bzw. das Gerät hat, wo das Depot gespeichert ist.

Ein persönliches Depot kann auf Netzwerkfreigaben, FTP-Servern, Wechselmedien, dem Acronis Online Backup Storage, Bandgeräten oder auf einem für die Maschine lokalen Laufwerk organisiert werden. Die Acronis Secure Zone wird als persönliches Depot betrachtet, das für alle Benutzer verfügbar ist, die sich am System anmelden können. Persönliche Depots werden automatisch erstellt, wenn Sie Backups zu einem der oberen Speicherorte durchführen.

Persönliche Depots können von lokalen Backup-Plänen bzw. Tasks verwendet werden. Zentrale Backup-Pläne können, mit Ausnahme der Acronis Secure Zone, keine persönlichen Depots verwenden.

Persönliche Depots erstellen

Mehrere Maschinen können sich auf denselben physikalischen Speicherort beziehen, beispielsweise auf denselben freigegebenen Ordern. Jede dieser Maschinen hat im Verzeichnisbaum **Depots** jedoch ihre eigene Verknüpfung. Benutzer, die ein Backup zu einem gemeinsam genutzten Ordner durchführen, können die Archive anderer Benutzer sehen und verwalten, abhängig von ihren

Zugriffsberechtigungen für diesen Ordner. Um die Identifikation von Archiven zu erleichtern, hat die Ansicht **Persönliches Depot** die Spalte **Besitzer**, die den Besitzer eines jeden Archivs zeigt. Um mehr über das Konzept der Besitzer zu erfahren, siehe Besitzer und Anmeldedaten (S. 35).

Metadaten

In jedem persönlichen Depot wird bei Backup-Durchführung ein Ordner namens **.meta** erstellt. Dieser Ordner enthält zusätzliche Informationen über die im Depot gespeicherten Archive und Backups, wie z.B. die Besitzer der Archive oder den Maschinen-Namen. Sollten Sie den .meta-Ordner einmal versehentlich löschen, dann wird er automatisch neu erstellt, sobald Sie das nächste Mal auf das Depot zugreifen. Einige Informationen, wie Besitzer- oder Maschinen-Namen, können jedoch verloren gehen.

7.1.3.1 Auf persönliche Depots anwendbare Aktionen

Zugriff auf Aktionen

1. Verbinden Sie die Konsole mit dem Management Server.
2. Klicken Sie im Fensterbereich **Navigation** auf **Depots** –> **Persönlich**.

Alle hier beschriebenen Aktionen werden durch Klicken auf die korrespondierenden Schaltflächen in der Depot-Symbolleiste ausgeführt. Sie können auf diese Aktionen auch über das Hauptmenüelement **[Depot-Name] Aktionen** zugreifen.

Anleitung zur Durchführung von Aktionen mit persönlichen Depots.

Aufgabe	**Lösung**
Persönliche Depots erstellen	Klicken Sie auf **Erstellen**. Die Prozedur zum Erstellen persönlicher Depots wird ausführlich im Abschnitt Ein persönliches Depot erstellen (S. 215) beschrieben.
Ein Depot bearbeiten	1. Wählen Sie das Depot. 2. Klicken Sie auf **Bearbeiten**. Auf der Seite **Persönliches Depot bearbeiten** können Sie den Depotnamen sowie die Informationen im Feld **Kommentare** bearbeiten.
Benutzerkonto für den Zugriff auf ein Depot ändern	Klicken Sie auf **Benutzer ändern**. Geben Sie im erscheinenden Dialogfenster die für den Zugriff auf das Depot benötigten Anmeldedaten ein.
Acronis Secure Zone erstellen	Klicken Sie auf **Acronis Secure Zone erstellen**. Die Prozedur zur Erstellung der Acronis Secure Zone ist ausführlich im Abschnitt Acronis Secure Zone erstellen (S. 218) erläutert.
Den Inhalt eines Depots durchsuchen	Klicken Sie auf **Durchsuchen**. Untersuchen Sie den gewählten Depot-Inhalt im erscheinenden Explorer-Fenster.
Ein Depot validieren	Klicken Sie auf **Validieren**. Sie gelangen zur Seite Validierung (S. 266) mit dem bereits als Quelle vorausgewählten Depot. Die Validierung des Depots überprüft alle in diesem Ordner gespeicherten Archive.

Ein Depot löschen	Klicken Sie auf **Löschen**. Tatsächlich entfernt die Löschaktion aus der Ansicht **Depots** nur die Verknüpfung zum entsprechenden Ordner. Der Ordner selbst bleibt unberührt. Sie haben die Möglichkeit, die im Ordner enthaltenen Archive zu behalten oder zu löschen.
Die Informationen der Depot-Tabelle aktualisieren	Klicken Sie auf **Aktualisieren**. Während Sie den Inhalt eines Depots einsehen, können Archive dem Depot hinzugefügt, aus diesem gelöscht oder modifiziert werden. Klicken Sie auf **Aktualisieren**, damit die neuesten Veränderungen für die Depot-Informationen berücksichtigt werden.

Ein persönliches Depot erstellen

So erstellen Sie ein persönliches Depot

1. Geben Sie im Feld **Name** die Bezeichnung für das zu erstellende Depot ein.
2. [Optional] Geben Sie im Feld **Kommentare** eine Beschreibung für das Depot ein.
3. Klicken Sie auf **Pfad** und spezifizieren Sie einen Pfad zu dem Ordner, der als Depot verwendet werden soll. Ein persönliches Depot kann auf Netzwerkfreigaben, FTP-Servern, entfernbaren Medien, dem Acronis Online Backup Storage, Bandgeräten oder auf einem für die Maschine lokalen Laufwerk organisiert werden.
4. [Optional] Falls das Depot auf einem Bandgerät erstellt wird:
    a. Klicken Sie auf **Laufwerke**, um das/die Bandlaufwerk(e) zu spezifizieren, welche(s) bei Backups zum Depot verwendet werden sollen. Standardmäßig werden alle verfügbaren Laufwerke verwendet. Klicken Sie auf **Nur die folgenden Laufwerke verwenden** und (de)aktivieren Sie die gewünschten Kontrollkästchen;
    b. Klicken Sie auf **Band-Pool** und spezifizieren Sie den Pool, dessen Bänder von dem Depot verwendet werden sollen. Standardmäßig ist der Pool **Acronis** vorausgewählt.
5. Klicken Sie auf **OK**. Als Ergebnis erscheint das erstellte Depot in der Gruppe **Persönlich** des Depot-Verzeichnisbaums.

Persönliche Depots zusammenführen und verschieben

Was ist, wenn ich ein existierendes Depot von einem Ort zu einem anderen verschieben muss?

Verfahren Sie wie folgt:

1. Stellen Sie sicher, dass kein Backup-Plan das betreffende Depot beim Verschieben der Dateien verwendet – oder deaktivieren Sie die entsprechenden Pläne. Siehe den Abschnitt 'Aktionen für Backup-Pläne und Tasks (S. 361)'.
2. Verschieben Sie den Depot-Ordner mit seinem kompletten Inhalt manuell, unter Verwendung des Datei-Managers eines anderen Herstellers.
3. Ein neues Depot erstellen.
4. Bearbeiten Sie die Backup-Pläne und Tasks: Stellen Sie ihre Zielortangaben auf das neue Depot um.
5. Löschen Sie das alte Depot.

Wie kann ich zwei Depots zusammenführen?

Angenommen, Sie benutzen zwei Depots *A* und *B*. Beide Depots werden von Backup-Plänen verwendet. Sie entscheiden, nur Depot *B* zu behalten, indem Sie alle Archive aus Depot *A* dorthin verschieben.

Zur Umsetzung verfahren Sie wie folgt:

1. Stellen Sie sicher, dass kein Backup-Plan das Depot *A* während der Zusammenführung verwendet – oder deaktivieren Sie die betreffenden Pläne temporär. Siehe den Abschnitt 'Aktionen für Backup-Pläne und Tasks (S. 361)'.
2. Verschieben Sie den Inhalt des Depots *A* manuell zum Depot *B* unter Verwendung des Datei-Managers eines anderen Herstellers.
3. Bearbeiten Sie die Backup-Pläne, die das Depot *A* benutzen: Stellen Sie die Zielortangaben auf Depot *B* um.
4. Wählen Sie im Depot-Verzeichnisbaum das Depot *B* aus, um zu überprüfen, dass die Archive angezeigt werden. Wenn nicht, klicken Sie auf **Aktualisieren**.
5. Löschen Sie das Depot *A*.

7.1.4 Den Standard-Cache-Ordner für Katalogdateien ändern

Katalogdateien werden normalerweise in Depots gespeichert. Beim Arbeiten mit Katalogdateien speichert Acronis Backup & Recovery 11.5 diese möglicherweise in einem lokalen Ordner auf einer verwalteten Maschine oder einem Management Server. Dies passiert in folgenden Fällen:

- Wenn ein Agent die zu einem nicht verwalteten Depot gesicherten Daten katalogisiert. Der Agent erstellt oder aktualisiert den Katalog lokal und kopiert ihn dann in das Depot.
- Wenn Backups auf einem Bandgerät gespeichert werden. Da ein Band eine lange Latenz beim wahlfreien Zugriff hat, wird der Katalog eines bandbasierten Depots immer auf der Maschine gespeichert, an die das Bandgerät angeschlossen ist.
- Beim Durchsuchen von auf einem FTP-Server gesicherten Daten in der Registerkarte **Datenanzeige**. Während des Durchsuchens bewahrt Acronis Backup & Recovery 11.5 eine vollständige Kopie des Datenkatalogs von einem FTP-Server auf einer verwalteten Maschine oder einem Management Server. Diese erfolgt, um einen schnelleren Zugriff auf den Datenkatalog zu ermöglichen.

Ein Cache-Ordner befindet sich standardmäßig auf dem Laufwerk, auf dem auch das Betriebssystem installiert ist. Die Speicherung mehrerer Katalogdateien an diesem Ort kann zu unzureichendem Speicherplatz führen. Daher möchten Sie möglicherweise den Ordnerpfad ändern.

Den Standard-Cache-Ordner ändern

Fügen Sie zu diesem Zweck unter Windows einen speziellen Parameter in die System-Registry ein oder modifizieren Sie die unter Linux die Konfigurationsdatei **MMS.config**.

Sollte der spezifizierte Ordner nicht existieren, dann wird Acronis Backup & Recovery 11.5 ihn automatisch erstellen, wenn die Katalogdateien das nächste Mal erstellt oder kopiert werden. Falls Sie Backups auf Bandgeräten speichern, sollten Sie den Ordner im Voraus erstellen, so dass die Daten nicht nochmals katalogisiert werden.

So spezifizieren Sie einen neuen Cache-Ordner unter Windows:

1. Fügen Sie den Schlüssel **Catalog** dem folgenden Registry-Schlüssel hinzu: **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\AMS\Configuration** (auf einem Management

Server) oder **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\MMS\Configuration** (auf einer verwalteten Maschine).

2. Fügen Sie den String-Wert **CatalogDir** hinzu.
3. Spezifizieren Sie einen neuen Ordnerpfad im String-Wert **CatalogDir**. Der Pfad muss mit einem Backslash (\) enden und darf 32765 Zeichen lang sein.

So spezifizieren Sie einen neuen Cache-Ordner unter Linux:

Fügen Sie folgendes Element innerhalb des Tags **`Configuration`** hinzu (in **/etc/Acronis/MMS.config**):

```
<key name="Catalog">
  <value name="CatalogDir" type="TString">"/home/Catalog/"</value>
</key>
```

Die Konfigurationsdatei sieht dann so aus:

```
<?xml version="1.0" encoding="UTF-8" ?>
<registry name="MMS">
  <key name="Configuration">
    ...
    <key name="Catalog">
      <value name="CatalogDir" type="TString">"/home/Catalog/"</value>
    </key>
  </key>
</registry>
```

Wobei **`/home/Catalog/`** ein neuer Ordnerpfad ist. Der Pfad muss mit einem Schrägstrich (Slash, /) enden und darf 32765 Zeichen lang sein.

Verschieben der Katalogdateien

Nach Änderung eines Cache-Ordners wird Acronis Backup & Recovery 11.5 die Katalogdateien weder zu dem neuen Ordner verschieben noch den alten Ordner entfernen.

Sollten Ihre Backups auf einem Bandgerät gespeichert sein, dann verschieben Sie die Katalogdateien zum neue Speicherort, so dass die Daten nicht nochmals katalogisiert werden müssen. Anderenfalls lassen Sie Acronis Backup & Recovery 11.5 die Katalogdateien neu erstellen oder kopieren.

Sie können den alten Ordner auf Wunsch auch löschen. Der Standardpfad des Cache-Ordners lautet folgendermaßen:

- In Windows XP und Server 2003: **%ALLUSERSPROFILE%\Application Data\Acronis\AMS\AMS\Catalog** (auf einem Management Server) oder **%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\MMS\Catalog** (auf einer verwalteten Maschine).
- In Windows Vista und späteren Versionen von Windows: **%PROGRAMDATA%\Acronis\AMS\AMS\Catalog** (auf einem Management Server) oder **%PROGRAMDATA%\Acronis\BackupAndRecovery\MMS\Catalog** (auf einer verwalteten Maschine)
- In Linux: **/var/lib/Acronis/BackupAndRecovery/MMS/Catalog/**

7.2 Acronis Secure Zone

Die Acronis Secure Zone ist ein sicheres Volume auf dem Laufwerksspeicherplatz einer verwalteten Maschine, in der Backup-Archive hinterlegt werden können, so dass die Wiederherstellung eines Laufwerks auf demselben Laufwerk erfolgen kann, auf dem sich auch die Backups selbst befinden.

Sollte das Laufwerk jedoch einen physikalischen Fehler haben, so gehen die Zone und alle dort aufbewahrten Archive verloren. Das ist der Grund, warum die Acronis Secure Zone nicht der einzige Ort sein sollte, wo Backups gespeichert werden. In Unternehmensumgebungen kann die Acronis Secure Zone als Zwischenspeicher für Backups betrachtet werden, wenn der üblicherweise verwendete Speicherort temporär nicht verfügbar ist oder über einen langsamen bzw. ausgelasteten Kanal angebunden ist.

Vorteile

Acronis Secure Zone:

- Ermöglicht die Wiederherstellung eines Laufwerks (wie einer Festplatte) zu demselben Laufwerk, auf dem die Laufwerk-Backups selbst hinterlegt sind.
- Bietet eine kosteneffektive und handliche Methode zum Schutz Ihrer Daten vor Softwarefehlern, Virusangriffen, Bedienungsfehlern u.a.
- Da es ein interner Archiv-Speicher ist, beseitigt er die Notwendigkeit, in jedem Fall für Backup oder Wiederherstellung ein separates Medium oder eine Netzwerkverbindung bereitstellen zu müssen. Diese Funktion ist besonders nützlich für mobile Benutzer.
- Kann als primäres Backup-Ziel dienen, wenn die Funktion Replikation von Backups (S. 106) verwendet wird.

Einschränkungen

- Die Acronis Secure Zone kann nicht auf einem dynamischen Laufwerk organisiert werden.

7.2.1 Acronis Secure Zone erstellen

Sie können die Acronis Secure Zone erstellen, während das Betriebssystem läuft oder Sie ein bootfähiges Medium benutzen.

Zur Erstellung der Acronis Secure Zone führen Sie die folgenden Schritte aus.

Speicherort und Größe

Laufwerk (S. 219)

Wählen Sie (sofern mehrere vorhanden sind) eine fest eingebaute Festplatte (oder ähnliches Laufwerk), auf dem die Zone erstellt werden soll. Die Acronis Secure Zone wird unter Verwendung von nicht zugeordnetem Speicherplatz oder auf Kosten freien Speicherplatzes der Partition erstellt.

Größe (S. 219)

Spezifizieren Sie die exakte Größe der Zone. Verschieben oder Größenveränderung einer gesperrten Partition, wie der aktuellen Betriebssystempartition, benötigen einen Neustart.

Sicherheit

Kennwort (S. 219)

[Optional] Schützen Sie die Acronis Secure Zone vor unerlaubtem Zugriff mit einem Kennwort. Das Kennwort wird bei jeder die Zone betreffende Aktion erfragt.

Klicken Sie auf OK, nachdem Sie die benötigten Einstellungen konfiguriert haben. Überprüfen Sie im Fenster Ergebnisbestätigung (S. 220) das erwartete Layout und klicken Sie auf OK, um die Erstellung der Zone zu starten.

7.2.1.1 Acronis Secure Zone Laufwerk

Die Acronis Secure Zone kann auf jeder fest installierten Festplatte (oder ähnlichem Laufwerk) liegen. Die Acronis Secure Zone wird immer am Ende des Laufwerks eingerichtet. Eine Maschine kann jedoch nur eine Acronis Secure Zone haben. Die Acronis Secure Zone wird unter Verwendung von 'nicht zugeordnetem' Speicherplatz oder auf Kosten freien Speicherplatzes der Volumes erstellt.

Die Acronis Secure Zone kann nicht auf einem dynamischen Laufwerk organisiert werden.

So weisen Sie der Acronis Secure Zone Speicherplatz zu

1. Wählen Sie (sofern mehrere vorhanden sind) eine fest eingebaute Festplatte (oder ähnliches Laufwerk), auf dem die Zone erstellt werden soll. Standardmäßig wird der 'nicht zugeordnete' sowie freie Speicherplatz aller Volumes des ersten aufgelisteten Laufwerks gewählt. Das Programm zeigt den insgesamt für die Acronis Secure Zone verfügbaren Speicherplatz an.
2. Wenn Sie der Zone mehr Speicherplatz zuweisen müssen, können Sie Volumes wählen, von denen freier Platz übernommen werden soll. Das Programm zeigt erneut den insgesamt für die Acronis Secure Zone verfügbaren Speicherplatz an, basierend auf Ihrer Auswahl. Sie können die exakte Größe der Zone im Fenster **Acronis Secure Zone Größe** (S. 219) einstellen.
3. Klicken Sie auf **OK**.

7.2.1.2 Acronis Secure Zone Größe

Geben Sie die Größe der Acronis Secure Zone ein oder ziehen Sie am Schieber, um eine Größe zwischen der minimalen und maximalen zu wählen. Die minimale Größe beträgt ca. 50 MB, abhängig von der Geometrie der Festplatte. Die maximale Größe entspricht dem nicht zugeordneten Festplattenplatz plus dem gesamten freien Platz aller im vorherigen Schritt gewählten Partitionen.

Beachten Sie Folgendes, wenn Sie Speicherplatz von der Boot- bzw. System-Partition verwenden müssen:

- Ein Verschieben oder eine Größenänderung der Partition, von der das System gegenwärtig bootet, verlangen einen Neustart.
- Die Verwendung des gesamten freien Speichers einer Systempartition kann dazu führen, dass das Betriebssystem instabil wird oder sogar nicht mehr startet. Stellen Sie also nicht die maximale Größe für die Zone ein, falls Sie die Boot- bzw. System-Partition gewählt haben.

7.2.1.3 Kennwort für die Acronis Secure Zone

Die Vergabe eines Kennwortes schützt die Acronis Secure Zone vor unerlaubtem Zugriff. Das Programm wird bei allen Aktionen, die die Zone und dort gespeicherte Archive betreffen, nach dem Kennwort fragen – wie etwa Backup und Wiederherstellung, Archiv-Validierung, Größenveränderung und Löschen der Zone.

So vergeben Sie ein Kennwort

1. Wählen Sie **Kennwort verwenden**.
2. Tippen Sie das neue Kennwort in das Feld **Kennwort eingeben** ein.
3. Tragen Sie das Kennwort im Eingabefeld **Kennwortbestätigung** erneut ein.
4. Klicken Sie auf **OK**.

So deaktivieren Sie ein Kennwort

1. Wählen Sie **Nicht verwenden**.
2. Klicken Sie auf **OK**.

7.2.1.4 Ergebnisbestätigung

Das Fenster **Ergebnisbestätigung** zeigt das erwartete Partitionslayout entsprechend der von Ihnen gewählten Einstellungen. Klicken Sie auf **OK**, falls Sie mit dem Layout einverstanden sind, worauf die Erstellung der Acronis Secure Zone startet.

So werden die Einstellungen umgesetzt

Die nachfolgende Erläuterung hilft Ihnen zu verstehen, welche Auswirkung die Erstellung der Acronis Secure Zone auf eine Festplatte hat, die mehrere Partitionen enthält.

- Die Acronis Secure Zone wird immer am Ende der Festplatte eingerichtet. Bei Kalkulation des endgültigen Partitionslayouts wird das Programm zuerst nicht zugeordneten, am Ende liegenden Festplattenplatz verwenden.
- Sollte der nicht zugeordnete Speicherplatz am Ende der Festplatte nicht ausreichen, jedoch zwischen den Partitionen noch nicht zugeordneter Speicherplatz vorhanden sein, so werden die Partitionen verschoben, um dem Endbereich mehr nicht zugeordneten Speicherplatz hinzuzufügen.
- Wenn dann der zusammengetragene nicht zugeordnete Speicherplatz immer noch nicht ausreicht, wird das Programm freien Speicherplatz von Partitionen beziehen, die Sie auswählen und deren Größe proportional verkleinern. Die Größenveränderung einer gesperrten Partition benötigt einen Neustart.
- Auf einem Laufwerk sollte jedoch genügend freier Platz vorhanden sein, so dass Betriebssystem und Anwendungen arbeitsfähig sind, z.B. zum Erstellen temporärer Dateien. Das Programm wird keine Partition verkleinern, deren freier Speicherplatz dadurch kleiner als 25% der Gesamtgröße wird. Nur wenn alle Partitionen der Festplatte mindestens 25% freien Speicherplatz haben, wird das Programm mit der proportionalen Verkleinerung der Partitionen fortfahren.

Daraus wird ersichtlich, dass es nicht ratsam ist, für die Zone die maximal mögliche Größe einzustellen. Sie haben am Ende dann auf keinem Laufwerk mehr freien Speicherplatz, was dazu führen kann, dass Betriebssystem und Anwendungen instabil arbeiten oder nicht mehr starten.

7.2.2 Die Acronis Secure Zone verwalten

Die Acronis Secure Zone wird als persönliches Depot (S. 489) betrachtet. Einmal auf einer verwalteten Maschine erstellt, ist die Zone stets in der Liste **Persönliche Depots** präsent. Die Acronis Secure Zone kann sowohl von zentralen Backup-Plänen als auch von lokalen Plänen verwendet werden.

Alle für Depots verfügbaren Aktionen zur Archiv-Verwaltung sind auch auf die Acronis Secure Zone anwendbar. Zu weiteren Informationen über Archiv-Verwaltungsaktionen siehe den Abschnitt 'Aktionen mit Archiven und Backups (S. 279)'.

7.2.2.1 Acronis Secure Zone vergrößern

So vergrößern Sie die Acronis Secure Zone

1. Klicken Sie auf der Seite **Acronis Secure Zone verwalten** auf **Vergrößern**.
2. Bestimmen Sie die Volumes, deren freier Speicher zur Vergrößerung der Acronis Secure Zone verwendet werden soll.
3. Spezifizieren Sie die neue Größe der Zone, indem Sie:

- am Schieber ziehen und so eine Größe zwischen dem gegenwärtigen und dem maximalen Wert wählen. Die maximale Größe entspricht dem nicht zugeordneten Festplattenspeicherplatz plus dem gesamten freien Speicher aller gewählten Partitionen;
- einen exakten Wert für die Größe der Acronis Secure Zone eingeben.

Bei Vergrößerung der Zone verfährt das Programm wie folgt:

- Zuerst wird es den nicht zugeordneten Festplattenspeicherplatz benutzen. Falls notwendig, werden Partitionen verschoben, jedoch nicht in ihrer Größe verändert. Das Verschieben einer gesperrten Partition benötigt einen Neustart.
- Sollte nicht genügend nicht zugeordneter Speicher vorhanden sein, so wird das Programm freien Speicherplatz von den ausgewählten Partitionen beziehen, deren Größe dabei proportional verkleinert wird. Die Größenveränderung einer gesperrten Partition benötigt einen Neustart.

Die Verkleinerung einer Systempartition auf ihre minimale Größe kann das Betriebssystem der Maschine am Booten hindern.

4. Klicken Sie auf **OK**.

7.2.2.2 Die Acronis Secure Zone verkleinern

So verkleinern Sie die Acronis Secure Zone

1. Klicken Sie auf der Seite **Acronis Secure Zone verwalten** auf **Verkleinern**.
2. Bestimmen Sie Volumes, die den frei werdenden Speicherplatz nach Verkleinerung der Zone zugesprochen bekommen.

   Der Speicherplatz wird gleichmäßig auf die entsprechenden Volumes verteilt, sofern Sie mehrere ausgewählt haben. Der freigegebene Bereich wird zu 'nicht zugeordneten' Speicherplatz, wenn Sie keine Volumes auswählen.
3. Spezifizieren Sie die neue Größe der Zone, indem Sie:
   - am Schieber ziehen und so eine Größe zwischen dem gegenwärtigen und minimalen Wert wählen. Die minimale Größe beträgt ca. 50 MB, abhängig von der Geometrie der Festplatte.
   - einen exakten Wert im Feld **Acronis Secure Zone Größe** eingeben.
4. Klicken Sie auf **OK**.

7.2.2.3 Eine Acronis Secure Zone löschen

So löschen Sie eine Acronis Secure Zone:

1. Klicken Sie auf der Seite **Acronis Secure Zone verwalten** auf den Befehl **Löschen**.
2. Wählen Sie im Fenster **Acronis Secure Zone löschen** diejenigen Volumes, denen Sie den durch die Zone freigegebenen Platz zuweisen wollen – klicken Sie anschließend auf **OK**.

   Der Speicherplatz wird gleichmäßig auf die entsprechenden Volumes verteilt, sofern Sie mehrere ausgewählt haben. Der freigegebene Bereich wird zu 'nicht zugeordneten' Speicherplatz, wenn Sie keine Volumes auswählen.

Nachdem Sie auf **OK** geklickt haben, beginnt Acronis Backup & Recovery 11.5 mit der Löschung der Zone.

7.3 Wechsellaufwerke

In diesem Abschnitt werden Besonderheiten beim Backup auf Wechsellaufwerke beschrieben.

Mit Wechsellaufwerk werden hier RDX- oder USB-Flash-Laufwerke (z.B. USB-Sticks) gemeint. Eine USB-Festplatte wird nicht als Wechsellaufwerk angesehen, außer es wird als solches vom Betriebssystem erkannt.

Unter Linux wird ein RDX- oder USB-Flash-Laufwerk als Wechsellaufwerk angesehen, wenn es über seinen Namen spezifiziert wird (beispielsweise **sdf:/**). Wird ein Laufwerk über seinen Mount-Punkt (beispielsweise **/mnt/backup**) spezifiziert, dann verhält es sich wie ein fest eingebautes Laufwerk.

Die Methode, nach der mit Wechselaufwerk-Bibliotheken (Multi-Cartridge-Geräte) gearbeitet wird, hängt vom Gerätetyp, dem Hersteller und der Konfiguration ab. Daher sollte jeder Fall individuell betrachtet werden.

Depots auf Wechsellaufwerken

Bevor Sie eine Maschine auf ein Wechsellaufwerk sichern, können Sie ein persönliches Depot erstellen (S. 215). Falls Sie nicht wollen, wird die Software automatisch ein persönliches Depot in dem für das Backup ausgewählten Laufwerksordner erstellen.

Beschränkungen

- Auf einem Bandgerät können keine zentrale Depots erstellt werden.
- Auf Wechsellaufwerken erstellte Depots haben keine Registerkarte **Datenanzeige** (S. 150).

Betriebsmodi von Wechsellaufwerken

Sie können bei Erstellung eines Backup-Plans wählen, ob Ihr Wechsellaufwerk als eingebautes Laufwerk oder wie ein Wechselmedium verwendet wird. Der Modus **Eingebautes Laufwerk** nimmt an, dass das Wechsellaufwerk immer an die Maschine angeschlossen sein wird. Der Modus **Wechselmedium** ist als Standard vorausgewählt.

Beim Backup unter Verwendung der Funktion **Backup jetzt** oder unter einem bootfähigen Medium wird das Wechsellaufwerk immer im Modus **Wechselmedium** verwendet.

Wenn Sie Backups mit dem Agenten für Exchange, dem Agenten für ESX(i) (Windows) oder dem Agenten für Hyper-V erstellen, dann wird das Wechsellaufwerk immer im Modus **Eingebautes Laufwerk** verwendet.

Der Unterschied zwischen diesen beiden Modi liegt hauptsächlich bei den Funktionen für Aufbewahrung und Replikation von Backups.

Funktionalität	**Eingebautes Laufwerk**	**Wechselmedium**
Falls der Speicherplatz zur Fortsetzung des Backups nicht ausreicht, wird die Software Sie auffordern:	...Speicherplatz manuell freizugeben.	...ein neues Medium einzulegen.
Sie können für die auf dem Gerät gespeicherten Backups Aufbewahrungsregeln (S. 107) einrichten.	Ja	Nein
Sie können zur Bereinigung des Archivs die Option '**Wenn nicht ausreichend Speicherplatz während des Backups vorhanden ist**' innerhalb des Backup-Schemas **Benutzerdefiniert** (S. 74) einrichten.	Ja	Nein
Vereinfachte Benennung (S. 83) von Backup-Dateien...	...ist nicht verfügbar.	...wird immer verwendet.

Das Replizieren von Backups (S. 106) *zu* einem Wechsellaufwerke ist möglich.	Ja	Nein
Sie können Backups auch *von* einem Wechsellaufwerk aus replizieren.	Nein	Nein
Ein Archiv mit mehreren Voll-Backups kann erstellt werden.	Ja	Nein. Die Software löscht vor Erstellung eines neuen Voll-Backups das komplette Archiv und startet danach ein neues.
Sie können jedes Backup eines jeden Archivs löschen.	Ja	Nein. Sie können nur ein Backup löschen, welches keine abhängigen Backups hat.

Da der Wechsellaufwerksmodus das Benennungsschema für Backup-Dateien bestimmt, erscheint das Kontrollkästchen **Backup-Dateien unter Verwendung des Archivnamens benennen...** nicht, wenn es sich beim Backup-Ziel um ein Wechsellaufwerk handelt.

7.4 Bandgeräte

Die folgenden Abschnitte erläutern ausführlich, wie Bandgeräte zur Speicherung von Backup-Archiven verwendet werden.

Sie können mit Bandgeräten arbeiten, falls Sie eine Advanced-Edition von Acronis Backup & Recovery 11.5 haben oder falls Sie ein Upgrade von Acronis Backup & Recovery 10 auf Acronis Backup & Recovery 11.5 durchgeführt haben.

7.4.1 Was ist ein Bandgerät?

Ein **Bandgerät** ist ein Oberbegriff für eine Bandbibliothek oder ein autonomes Bandlaufwerk.

Eine **Bandbibliothek** (Roboterbibliothek) ist eine Speichereinrichtung mit hoher Kapazität, die aus den folgenden Komponenten besteht:

- einem oder mehreren Bandlaufwerken
- mehreren (bis zu mehreren Tausend) Schächten zur Aufnahme von Bändern
- einem oder mehreren Wechslern (Robotermechanismen), deren Aufgabe im Wechseln der Bänder zwischen den Schächten und den Bandlaufwerken besteht.

Es können noch weitere Komponenten enthalten sein, etwa ein Barcode-Leser oder Barcode-Drucker.

Ein **Autoloader** ist ein spezieller Fall einer Bandbibliothek. Er enthält ein Laufwerk, mehrere Schächte, einen Wechsler und (optional) einen Barcode-Leser.

Ein **autonomes Bandlaufwerk** (auch **Streamer** genannt) hat einen Schacht und kann jeweils nur ein Band aufnehmen.

7.4.2 Überblick der Band-Unterstützung

Die Acronis Backup & Recovery 11.5 Agenten können Daten per Backup entweder direkt oder über einen Acronis Backup & Recovery 11.5 Storage Node (S. 18) auf Band sichern. In beiden Fällen ist eine vollautomatische Steuerung des Bandgerätes gewährleistet. Wird ein Bandgerät mit mehreren Laufwerken an einen Storage Node angeschlossen, dann können mehrere Maschinen gleichzeitig Backups auf Band durchführen.

7.4.2.1 Kompatibilität mit RSM und Dritthersteller-Software

Koexistenz mit Dritthersteller-Software

Acronis Backup & Recovery 11.5 kann nicht mit Bändern auf Maschinen arbeiten, auf denen Dritthersteller-Software mit proprietären Tools zur Bandverwaltung installiert ist. Damit Acronis Backup & Recovery 11.5 auf solch einer Maschine doch mit Bändern arbeiten kann, müssen Sie die Bandverwaltungssoftware des Drittherstellers deinstallieren oder deaktivieren.

Interaktion mit RSM

Anders als Acronis Backup & Recovery 10 verwendet Acronis Backup & Recovery 11.5 den Windows Removable Storage Manager (RSM, Wechselmedien-Manager) nicht mehr. Acronis Backup & Recovery 11.5 schreibt bei einem Upgrade von Acronis Backup & Recovery 10 die notwendigen Informationen vom RSM im neuen Format in seine eigene Datenbank.

Bei Erkennung eines Bandgerätes (S. 233) deaktiviert Acronis Backup & Recovery 11.5 dieses vom RSM (außer es wird gerade durch andere Software blockiert). Solange Acronis Backup & Recovery 11.5 mit dem Bandgerät arbeiten soll, sollten Sie sicherstellen, dass weder ein Benutzer noch eine Dritthersteller-Software das Gerät wieder für den RSM aktiviert. Sollte das Bandgerät für den RSM aktiviert worden sein, dann wiederholen Sie die Bandgeräterkennung.

7.4.2.2 Unterstützte Hardware

Acronis Backup & Recovery 11.5 unterstützt externe SCSI-Geräte. Das sind Geräte, die per Fibre Channel angebunden sind oder SCSI, iSCSI bzw. Serial Attached SCSI (SAS) als Schnittstelle verwenden. Acronis Backup & Recovery 11.5 unterstützt außerdem per USB angeschlossene Bandgeräte.

Unter Windows kann Acronis Backup & Recovery 11.5 Backups auch dann auf ein Bandgerät erstellen, wenn die Treiber für den Wandler des Gerätes nicht installiert sind. Ein solches Bandgerät wird im **Geräte-Manager** als **Unbekannter Medienwechsler** angezeigt. Treiber für die Laufwerke des Gerätes müssen jedoch installiert sein. Unter Linux und bootfähigen Medien sind Backups auf ein Bandgerät ohne Treiber nicht möglich.

Eine Erkennung von per IDE oder SATA angebunden Geräten wird nicht garantiert. Sie hängt davon ab, ob im Betriebssystem die korrekten Treiber installiert wurden.

7.4.2.3 Bandverwaltungsdatenbank

Acronis Backup & Recovery 11.5 speichert Informationen über alle an eine Maschine angeschlossenen Bandgeräte in der Bandverwaltungsdatenbank. Der Standardpfad für die Datenbank lautet folgendermaßen:

- In Windows XP/Server 2003: **%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\ARSM\Database**.
- In Windows Vista und späteren Versionen von Windows: **%PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database**.
- In Linux: **/var/lib/Acronis/BackupAndRecovery/ARSM/Database**.

Die Datenbankgröße hängt von der Zahl der auf Bändern gespeicherten Archive ab – wobei etwa 10 MB auf einhundert Archive kommen. Die Datenbank kann recht groß werden, wenn die Bandbibliothek tausende Archive enthält. In diesem Fall könnten Sie erwägen, die Band-Datenbank auf einem anderen Volume zu speichern.

So verlagern Sie die Datenbank unter Windows:

1. Stoppen Sie den Acronis Removable Storage Management Service.
2. Verschieben Sie alle Dateien vom vorgegebenen Speicherort zum neuen Speicherort.
3. Fügen Sie die nachfolgend beschriebenen Registry-Schlüssel hinzu. Spezifizieren Sie den Pfad zum neuen Speicherort im Registry-Wert **ArsmDmlDbProtocol**.

   Registry-Schlüssel: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings

   Registry-Wert: **ArsmDmlDbProtocol**

   Mögliche Datenwerte: Jede Zeichenkette, 0 bis 32.765 Zeichen lang.

   Beschreibung: Spezifiziert den Ordner, in dem die Bandverwaltungsdatenbank gespeichert wird.
4. Starten Sie den Acronis Removable Storage Management Service.

So verlagern Sie die Datenbank unter Linux:

1. Stoppen Sie den Dienst **`acronis_rsm`**.
2. Verschieben Sie alle Dateien vom vorgegebenen Speicherort zum neuen Speicherort.
3. Öffnen Sie die Konfigurationsdatei **/etc/Acronis/ARSM.config** in einem Text-Editor.
4. Suchen Sie nach der Zeile **`<value name="ArsmDmlDbProtocol" type="TString">`**.
5. Ändern Sie den Pfad unter dieser Ziele.
6. Speichern Sie die Datei.
7. Starten Sie den Dienst **`acronis_rsm`**.

7.4.2.4 Besonderheiten von Backups auf Bändern

Backup-Optionen

Sie können die Backup-Optionen für die **Bandverwaltung** (S. 138) konfigurieren, um festzulegen:

- Wann ein Band ausgeworfen werden soll.
- Ob ein freies Band für jedes vollständige, inkrementelle oder differentielle Backup verwendet werden soll.
- Ob ein Band überschrieben werden soll, wenn ein neues Voll-Backup erstellt wird (nur für autonome Bandlaufwerke).
- Ob zum Backup einer jeden Maschine ein separater Bandsatz verwendet werden soll.
- Ob das Datei-Recovery für auf Bändern gespeicherte Laufwerk-Backups aktiviert werden soll.

Backup-Schemata

Schema 'Einfach'

Wenn Sie das Backup-Schema 'Einfach' (S. 69) verwenden, können nur Voll-Backups auf Bändern erstellt werden. Der Grund ist, dass auf Bändern vorliegende Backups nicht konsolidiert (S. 492) werden können. Wenn Sie die Option zur Erstellung inkrementeller Backups hätten, könnten Sie keines dieser Backups löschen.

Die Schemata 'Großvater-Vater-Sohn' und 'Türme von Hanoi'

Standardmäßig erstellen die Backup-Schemata Großvater-Vater-Sohn (S. 70) und Türme von Hanoi (S. 76) nur Voll-Backups auf Bändern. Das hilft der Software, jedes Backup enstprechend der Definition des Backup-Schemas planmäßig zu löschen.

Sie können auf Wunsch die Standardeinstellungen zur Erstellung vollständiger, inkrementeller und differentieller Backups ändern. Falls Sie beispielsweise nur einige Bänder haben, Ihre Voll-Backups aber ziemlich groß sind, dann möchten Sie vielleicht Speicherplatz auf den Bändern einsparen.

Jede Ebene der oberen Schemata verwendet einen separaten Bandsatz innerhalb desselben Band-Pools. Das bedeutet, dass die Software entweder nur ein Band nehmen kann, welches zu einem bestimmten Bandsatz gehört – oder ein freies Band (wenn der Speicherplatz des aktuell verwendeten Bands zur Neige geht). Das hilft dabei, die Menge an genutzten Bändern zu minimieren, weil Bänder mit inkrementellen und differentiellen Backups öfter befüllt und neu beschrieben werden als Bänder mit Voll-Backups.

Benutzerdefiniertes Schema

Konfigurieren Sie das benutzerdefinierte Schema so, dass es vollständige Backups mit angemessener Häufigkeit erstellt. Falls Sie Aufbewahrungsregeln spezifizieren, kann die Software anderenfalls die Bänder nicht angemessen überschreiben.

In den Aufbewahrungsregeln des benutzerdefinierten Backup-Schemas (S. 74) ist die Option **Falls ein zu verschiebendes oder löschendes Backup Abhängigkeiten hat: Backups konsolidieren** deaktiviert. Nur die Option **Backup bewahren, bis alle abhängigen Backups gelöscht werden** steht zur Verfügung. Der Grund ist, dass auf Bändern vorliegende Backups nicht konsolidiert (S. 492) werden können.

7.4.2.5 Parallele Aktionen

Acronis Backup & Recovery 11.5 kann Aktionen mit verschiedenen Komponenten eines Bandgerätes gleichzeitig durchführen. Sie können während einer Aktion (Backup, Recovery, erneutes Scannen (S. 238) oder Löschen (S. 237)), die ein Bandlaufwerk verwendet, eine Aktion starten, die einen Wechsler verwendet (ein Band zu einem anderen Schacht verschieben (S. 237) oder ein Band auswerfen (S. 237)). Falls Ihre Bandbibliothek mehr als ein Laufwerk hat, können Sie zudem eine Aktion starten, die eines der Laufwerke nutzt, während eine Aktion mit einem anderen abläuft. Mehrere Maschinen können beispielsweise gleichzeitig sichern oder wiederherstellen – unter Verwendung verschiedener Laufwerke derselben Bandbibliothek.

Die Aktion zur Erkennung neuer Bandgeräte (S. 233) kann gleichzeitig mit jeder anderen Aktion durchgeführt werden. Während einer Inventarisierung (S. 239) ist – mit Ausnahme der Aktion 'Neue Bandgeräte ermitteln' – keine andere Aktion verfügbar.

Aktionen, die nicht parallel ausgeführt werden können, werden in eine Warteschlange gestellt.

7.4.2.6 Beschränkungen

Bei Verwendung von Bandgeräten gelten folgende Beschränkungen:

1. Eine Konsolidierung (S. 492) von Backups, die auf Bändern liegen, ist nicht möglich. Als Folge hat die Verwendung von Backup-Schemata gewisse Besonderheiten (S. 225).
2. Eine Deduplizierung (S. 488) von Backups, die auf Bändern liegen, ist nicht möglich.
3. Eine vereinfachte Benennung von Backup-Dateien (S. 83) ist für auf Bändern gespeicherte Backups nicht möglich.
4. Sie können unter einem Betriebssystem keine auf Bändern gespeicherten Backups wiederherstellen, wenn für die Recovery-Aktion ein Neustart des Betriebssystems erforderlich ist. Verwenden Sie zur Durchführung einer solchen Wiederherstellung ein bootfähiges Medium.

5. Von Laufwerk-Backups, die mit Acronis Backup & Recovery 11 Update 0 (Build 17318) oder früher erstellt wurden, können keine Dateien wiederhergestellt werden.

   Von Laufwerk-Backups, die mit Acronis Backup & Recovery 11 Update 0.5 (Build 17437) erstellt wurden, können nur dann Dateien wiederhergestellt werden, wenn Sie die Bändern, auf denen das Backup liegt, erneut scannen (S. 238).

   Der Optionswert **Datei-Recovery für auf Bändern gespeicherte Laufwerk-Backups aktivieren** (S. 138) bestimmt, ob Dateien und Ordner von Laufwerk-Backups wiederhergestellt werden können, die mit Acronis Backup & Recovery 11.5 gesichert wurden.
6. Sie können jedes auf Bändern gespeicherte Backup bzw. Archiv validieren (S. 266), aber Sie können keine Validierung eines kompletten bandbasierten Depots oder Bandgerätes durchführen.
7. Sie können bandbasierte Depots nicht anschließen (S. 211) oder trennen.
8. Ein verwaltetes bandbasiertes Depot kann nicht per Verschlüsselung geschützt werden. Verschlüsseln Sie stattdessen Ihre Archive.
9. Sie können ein verwaltetes bandbasiertes Depot (S. 206) nicht mit der Eigenschaft 'Abwärtskompatibilität' erstellen. Dies bedeutet, dass Agenten von Acronis Backup & Recovery 10 keine Backups zu verwalteten bandbasierten Depots von Acronis Backup & Recovery 11.5 durchführen können.
10. Die Software kann ein Backup nicht gleichzeitig auf mehrere Bänder schreiben – oder mehrere Backups mittels desselben Laufwerks auf dasselbe Band.
11. Es werden keine Geräte unterstützt, die das 'Network Data Management Protocol' (NDMP) verwenden.
12. Es werden keine Barcode-Drucker unterstützt.

7.4.2.7 Lesbarkeit von mit älteren Acronis-Produkten beschriebenen Bändern

Die nachfolgende Tabelle fasst die Lesbarkeit von Bändern in Acronis Backup & Recovery 11.5 zusammen, die durch die Produktfamilie Acronis True Image Echo, Acronis True Image 9.1, Acronis Backup & Recovery 10 und Acronis Backup & Recovery 11 beschrieben wurden. Die Tabelle illustriert außerdem die Kompatibilität von Bändern, die durch verschiedene Komponenten von Acronis Backup & Recovery 11.5 beschrieben wurden.

			... ist lesbar auf einem Bandgerät, angeschlossen an eine Maschine mit...			
			ABR11.5 Bootmedium	ABR11.5 Agent für Windows	ABR11.5 Agent für Linux	ABR11.5 Storage Node
Band, beschrieben auf einem lokal angeschlossenen Bandgerät (Bandlaufwerk oder -bibliothek), durch...	Bootfähiges Medium	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/11.5	+	+	+	+
	Agent für Windows	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/11.5	+	+	+	+
	Agent für Linux	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/11.5	+	+	+	+

Band, beschrieben auf einem Bandgerät, durch...	Backup Server	9.1	-	-	-	-
		Echo	-	-	-	-
	Storage Node	ABR10	+	+	+	+
		ABR11/11.5	+	+	+	+

7.4.3 Erste Schritte bei Verwendung eines Bandgeräts

7.4.3.1 Backup einer Maschine zu einem direkt angeschlossenen Bandgerät

Voraussetzungen

- Das Bandgerät ist gemäß den Herstelleranweisungen mit der Maschine verbunden.
- Der Acronis Backup & Recovery 11.5 Agent ist auf der Maschine installiert.

Vor dem Backup

1. Beladen Sie das Bandgerät mit Bändern.
2. Verbinden Sie die Konsole mit der Maschine.
3. Klicken Sie im Verzeichnisbaum **Navigation** auf den Befehl **Bandverwaltung**.
4. Klicken Sie auf **Bandgeräte erkennen**.
5. Falls Ihr Bandgerät ein autonomes Laufwerk ist, dann überspringen Sie diesen Schritt. Anderenfalls tun Sie Folgendes:
   a. Klicken Sie auf **Inventarisierung**, damit die geladenen Bänder erkannt werden. Wählen Sie die Inventarisierungsmethode '**Vollständig**'. Aktivieren Sie nicht das Kontrollkästchen **Neu erkannte Bänder vom Pool 'Unbekannte Bänder' oder 'Importierte Bänder' zum Pool 'Freie Bänder' verschieben**.

      Ergebnis: Die geladenen Bänder wurden zu den passenden Pools verschoben, so wie im Abschnitt 'Inventarisierung (S. 239)' spezifiziert.

      Die vollständige Inventarisierung eines kompletten Bandgerätes kann viel Zeit benötigen.

   b. Falls die geladenen Bänder an den Pool **Unbekannte Bänder** oder **Importierte Bänder** übertragen wurden und Sie diese für Backups nutzen wollen, dann verschieben (S. 236) Sie diese Bänder manuell zum Pool **Freie Bänder**.

      *An den Pool **Importierte Bänder** übertragene Bänder enthalten Backups, die von Acronis-Software auf die Bänder geschrieben wurden. Bevor Sie solche Bänder in den Pool **Freie Bänder** verschieben, sollten Sie sicherstellen, dass Sie diese Backups nicht mehr benötigen.*

Backup

Klicken Sie im Menü **Aktionen** auf **Backup jetzt** oder **Backup-Plan erstellen**. Konfigurieren (S. 58) Sie die Backup-Einstellungen. Wählen Sie bei Konfiguration des Backup-Ziels das Bandgerät aus.

Ergebnis

- Die resultierenden Backups werden in ein automatisch erstelltes persцnliches Depot (S. 242) hinterlegt. Der Zugriff auf das Depot ist über den Punkt **Depots** im Verzeichnisbaum **Navigation** möglich. Jedes Mal, wenn Sie das Bandgerät als Backup-Ziel wählen, werden die Backups zu demselben Depot gespeichert.
- Bänder mit Backups werden zum **Acronis**-Pool verschoben.

7.4.3.2 Backup zu einem Bandgerät, das an einen Storage Node angeschlossen ist

Voraussetzungen

- Ein Acronis Backup & Recovery 11.5 Storage Node wurde dem Management Server hinzugefьgt (S. 250).
- Das Bandgerät ist gemäß den Herstelleranweisungen mit dem Storage Node verbunden.

Vor dem Backup

1. Beladen Sie das Bandgerät mit Bändern.
2. Verbinden Sie die Konsole mit dem Management Server.
3. Klicken Sie im Verzeichnisbaum **Navigation** auf den Befehl **Bandverwaltung**. Wählen Sie den Storage Node, an den Ihr Bandgerät angeschlossen ist.
4. Klicken Sie auf **Bandgeräte erkennen**.
5. Falls Ihr Bandgerät ein autonomes Laufwerk ist, dann überspringen Sie diesen Schritt. Anderenfalls tun Sie Folgendes:
   a. Klicken Sie auf **Inventarisierung**, damit die geladenen Bänder erkannt werden. Wählen Sie die Inventarisierungsmethode '**Vollständig**'. Aktivieren Sie nicht das Kontrollkästchen **Neu erkannte Bänder vom Pool 'Unbekannte Bänder' oder 'Importierte Bänder' zum Pool 'Freie Bänder' verschieben**.

      Ergebnis: Die geladenen Bänder wurden zu den passenden Pools verschoben, so wie im Abschnitt 'Inventarisierung (S. 239)' spezifiziert.

      Die vollständige Inventarisierung eines kompletten Bandgerätes kann viel Zeit benötigen.

   b. Falls die geladenen Bänder an den Pool **Unbekannte Bänder** oder **Importierte Bänder** übertragen wurden und Sie diese für Backups nutzen wollen, dann verschieben (S. 236) Sie diese Bänder manuell zum Pool **Freie Bänder**.

      *An den Pool **Importierte Bänder** übertragene Bänder enthalten Backups, die von Acronis-Software auf die Bänder geschrieben wurden. Bevor Sie solche Bänder in den Pool **Freie Bänder** verschieben, sollten Sie sicherstellen, dass Sie diese Backups nicht mehr benötigen.*

   c. Entscheiden Sie, ob Ihre Backups auf Bänder erfolgen sollen, die sich im vorgegebenen **Acronis**-Pool (S. 233) befinden – oder ob Sie einen neuen Pool erstellen (S. 234) wollen.

      Details: Wenn Sie mehrere Pools haben, dann können Sie damit auch für jede Maschine oder Unternehmensabteilung einen separaten Bandsatz verwenden. Durch die Verwendung mehrerer Pools können Sie verhindern, dass Backups, die von unterschiedlichen Backup-Plänen erstellt wurden, auf einem Band gemischt werden.

   d. Überspringen Sie diesen Schritt, falls Sie den **Acronis**-Pool gewählt haben oder für den neuen Pool aktiviert haben, dass dieser bei Bedarf Bänder aus dem Pool **Freie Bänder** nehmen soll.

      Verschieben Sie anderenfalls Bänder vom Pool **Freie Bänder** zu dem neuen Pool.

      Tipp: Um zu erfahren, ob ein Pool Bänder aus dem Pool **Freie Bänder** entnehmen kann, klicken Sie auf diesen entsprechenden Pool und wählen dann den Befehl **Details**.
6. Klicken Sie im Verzeichnisbaum **Navigation** auf **Storage Nodes**. Wählen Sie den Storage Node, an den Ihr Bandgerät angeschlossen ist, und klicken Sie dann auf **Depot erstellen**. Fahren Sie fort wie im Abschnitt 'Ein zentrales, verwaltetes Depot erstellen (S. 206)' beschrieben. Wählen Sie in der Liste **Band-Pool** denjenigen Pool, zu dessen Verwendung Sie sich in Schritt 5c entschlossen haben.

   Die Erstellung eines zentralen Depots ist zwingend, wenn das Bandgerät an den Storage Node angeschlossen ist.

Backup

Klicken Sie im Menü **Aktionen** auf **Backup jetzt** oder **Backup-Plan erstellen**. Konfigurieren (S. 396) Sie die Backup-Einstellungen für eine oder mehrere Maschinen. Wählen Sie bei Konfiguration des Backup-Ziels das erstellte Depot aus.

Ergebnis

- Die resultierenden Backups werden sich in dem von Ihnen erstellten Depot befinden.

Tipps zur weiteren Nutzung der Bandbibliothek

- Sie müssen nicht jedes Mal, wenn Sie ein neues Band laden, eine vollständige Inventarisierung durchführen. Folgen Sie zur Zeitersparnis der im Abschnitt 'Inventarisierung (S. 239)' beschriebenen Prozedur (unter 'Schnelle und vollständige Inventarisierung kombinieren').
- Sie können auch andere Depots (S. 242) auf derselben Bandbibliothek erstellen und jedes davon als Backup-Ziel auswählen.

7.4.3.3 Wiederherstellung unter einem Betriebssystem von einem Bandgerät

So führen Sie eine Recovery-Aktion unter einem Betriebssystem von einem Bandgerät aus:

1. Verbinden Sie die Konsole mit der Maschine, die Sie wiederherstellen wollen.
2. Klicken Sie im Menü **Aktionen** auf den Befehl **Recovery**.
3. Klicken Sie auf **Daten wählen**, gehen Sie anschließend zu **Datenpfad** und klicken Sie dann auf **Durchsuchen**.
4. Wählen Sie das Depot, welches das Backup mit den wiederherzustellenden Daten enthält, klicken Sie auf **OK** und dann auf **Archiv-Anzeige**.
5. Wählen Sie zuerst das Backup und dann die Daten, die Sie wiederherstellen wollen. Nachdem Sie auf **OK** geklickt haben, wird Ihnen auf der Seite **Recovery** eine Liste der für die Wiederherstellung benötigten Bänder angezeigt. Fehlende Bänder sind ausgegraut dargestellt. Sollte Ihr Bandgerät noch leere Schächte haben, dann laden Sie diese Bänder in das Gerät.
6. Konfigurieren (S. 146) Sie andere Recovery-Einstellungen.
7. Klicken Sie auf **OK**, um die Wiederherstellung zu starten.
8. Sollte eines der benötigten Bänder aus irgendeinem Grund nicht geladen sein, dann wird Ihnen die Software eine Nachricht mit dem Identifier des erforderlichen Bandes anzeigen. Laden Sie das Band und klicken Sie dann auf **Wiederholen**, um mit der Wiederherstellung fortzufahren.

Was, wenn ich keine auf Bändern gespeicherten Backups sehen kann?

Das kann bedeuten, dass die Datenbank mit den Bandinhalten aus irgendeinem Grund verloren gegangen ist oder beschädigt wurde.

Tun Sie Folgendes, um die Datenbank wiederherzustellen:

Falls das Backup auf der Maschine vorhanden ist

1. Wählen Sie, nachdem Sie auf **Recovery** geklickt haben, zuerst **Datenauswahl** und dann **Durchsuchen**.
2. Klicken Sie doppelt auf **Bandgeräte**. Das System erfragt eine Bestätigung der Bandgerät-Erkennung. Klicken Sie auf **Ja**.
3. Wählen Sie, nachdem die erkannten Bandgeräte im Verzeichnisbaum erscheinen, auf das benötigte Gerät und klicken Sie dann auf **OK**. Das System erfragt eine Bestätigung für die Aktion zum erneuten Scannen. Klicken Sie auf **Ja**.

4. Lassen Sie den Pool **Unbekannte Bänder** erneut scannen (S. 238). Als Ergebnis erhalten Sie die Inhalte des geladenen Bandes (bzw. der Bänder).
5. Falls irgendwelche der ermittelten Backups auf anderen Bändern fortgesetzt werden, die bisher noch nicht neu eingescannt wurden, dann laden Sie diese Bänder bei entsprechender Aufforderung und scannen Sie auch diese neu ein.
6. Danach können Sie das benötigte Backup auswählen.

Falls sich das Backup auf einem Storage Node befindet

1. Verbinden Sie die Konsole mit dem Management Server.
2. Erkennen Sie die Bandgerдte (S. 233).
3. Führen Sie eine schnelle Inventarisierung (S. 239) durch.

   Aktivieren Sie während der Inventarisierung nicht *das Kontrollkästchen* ***Neu erkannte Bänder vom Pool 'Unbekannte Bänder' oder 'Importierte Bänder' zum Pool 'Freie Bänder' verschieben****. Falls dieses Kontrollkästchen aktiviert ist, können Sie alle Ihre Backups verlieren.*

4. Erstellen Sie ein verwaltetes Depot (S. 242) auf dem Bandgerät.
5. Lassen Sie den Pool **Unbekannte Bänder** erneut scannen (S. 238). Als Ergebnis erhalten Sie die Inhalte des geladenen Bandes (bzw. der Bänder).
6. Falls irgendwelche der ermittelten Backups auf anderen Bändern fortgesetzt werden, die bisher noch nicht neu eingescannt wurden, dann laden Sie diese Bänder bei entsprechender Aufforderung und scannen Sie auch diese neu ein.

7.4.3.4 Wiederherstellung mit einem bootfähigen Medium von einem lokal angebundenen Bandgerät

So führen Sie eine Wiederherstellung mit einem bootfähigen Medium von einem lokal angebundenen Bandgerät aus:

1. Laden Sie die für die Wiederherstellung benötigten Bänder in das Bandgerät.
2. Booten Sie die Maschine mit dem bootfähigen Medium.
3. Klicken Sie auf **Acronis Backup & Recovery 11.5** und dann auf **Diese Maschine lokal verwalten**. Überspringen Sie diesen Schritt, falls Sie ein WinPE-basiertes Medium verwenden.
4. Sollte das Bandgerät per iSCSI-Schnittstelle angebunden sein, dann konfigurieren Sie das Gerät wie unter 'iSCSI- und NDAS-Gerдte konfigurieren' (S. 295) beschrieben.
5. Klicken Sie auf **Recovery**.
6. Klicken Sie auf **Daten wählen** und dann auf **Durchsuchen**.
7. Klicken Sie doppelt auf **Bandgeräte**. Das System erfragt eine Bestätigung der Bandgerät-Erkennung. Klicken Sie auf **Ja**.
8. Wählen Sie, nachdem die erkannten Bandgeräte im Verzeichnisbaum erscheinen, das benötigte Gerät. Das System erfragt eine Bestätigung der Aktion 'Erneut scannen'. Klicken Sie auf **Ja**.
9. Wählen Sie den Pool **Unbekannte Bänder**.
10. Wählen Sie die erneut zu scannenden Bänder. Aktivieren Sie zur Wahl aller Bänder des Pools das Kontrollkästchen neben dem Spaltenkopf **Bandname**.
11. Sollten die Bänder ein kennwortgeschütztes Archiv enthalten, dann aktivieren Sie das entsprechende Kontrollkästchen und spezifizieren Sie das Kennwort des Archivs im Feld **Kennwort**. Ohne oder bei falscher Angabe des Kennwortes werden die Archive nicht erkannt. Beachten Sie dies, falls Sie nach dem erneuten Scannen keine Archive sehen.

Tipp: Sollten die Bänder mehrere kennwortgeschützte Archive enthalten, die wiederum verschiedene Kennwörter verwenden, dann müssen Sie das erneute Scannen mehrfach wiederholen, um jedes Kennwort entsprechend einzugeben.

12. Klicken Sie auf **Start**, damit das erneute Scannen beginnt. Als Ergebnis erhalten Sie die Inhalte des geladenen Bandes (bzw. der Bänder).
13. Falls irgendwelche der ermittelten Backups auf anderen Bändern fortgesetzt werden, die bisher noch nicht neu eingescannt wurden, dann laden Sie diese Bänder bei entsprechender Aufforderung und scannen Sie auch diese neu ein.
14. Klicken Sie auf **OK**, nachdem das erneute Scannen abgeschlossen ist.
15. Wählen Sie in der **Archiv-Anzeige** das Backup für die Recovery-Aktion aus und wählen Sie dann die wiederherzustellenden Daten. Nachdem Sie auf **OK** geklickt haben, wird Ihnen auf der Seite **Recovery** eine Liste der für die Wiederherstellung benötigten Bänder angezeigt. Fehlende Bänder sind ausgegraut dargestellt. Sollte Ihr Bandgerät noch leere Schächte haben, dann laden Sie diese Bänder in das Gerät.
16. Konfigurieren (S. 146) Sie andere Recovery-Einstellungen.
17. Wählen Sie **OK**, um die Wiederherstellung zu starten.
18. Sollte eines der benötigten Bänder aus irgendeinem Grund nicht geladen sein, dann wird Ihnen die Software eine Nachricht mit dem Identifier des erforderlichen Bandes anzeigen. Laden Sie das Band und klicken Sie dann auf **Wiederholen**, um mit der Wiederherstellung fortzufahren.

7.4.3.5 Wiederherstellung mit einem bootfähigen Medium von einem Bandgerät, das an einem Storage Node angeschlossen ist

So führen Sie eine Wiederherstellung einem bootfähigen Medium von einem Bandgerät aus, das an einem Storage Node angeschlossen ist:

1. Laden Sie die für die Wiederherstellung benötigten Bänder in das Bandgerät.
2. Booten Sie die Maschine mit dem bootfähigen Medium.
3. Klicken Sie auf **Acronis Backup & Recovery 11.5** und dann auf **Diese Maschine lokal verwalten**. Überspringen Sie diesen Schritt, falls Sie ein WinPE-basiertes Medium verwenden.
4. Klicken Sie auf **Recovery**.
5. Klicken Sie auf **Datenauswahl** und klicken Sie dann auf **Durchsuchen**.
6. Geben Sie in die Box **Pfad** die Zeichenfolge '`bsp://`<Storage Node-Adresse>**/**<Depot-Name>**/**' ein – wobei <Storage Node-Adresse> der IP-Adresse des Storage Nodes entspricht, der das benötigte Backup enthält und <Depot-Name> dem Namen des Depots entspricht. Klicken Sie auf **OK** und spezifizieren Sie die Anmeldedaten für das Depot.
7. Wählen Sie zuerst das Backup und dann die Daten, die Sie wiederherstellen wollen. Nachdem Sie auf **OK** geklickt haben, wird Ihnen auf der Seite **Recovery** eine Liste der für die Wiederherstellung benötigten Bänder angezeigt. Fehlende Bänder sind ausgegraut dargestellt. Sollte Ihr Bandgerät noch leere Schächte haben, dann laden Sie diese Bänder in das Gerät.
8. Konfigurieren (S. 146) Sie noch andere Recovery-Einstellungen.
9. Wählen Sie **OK**, um die Wiederherstellung zu starten.
10. Sollte eines der benötigten Bänder aus irgendeinem Grund nicht geladen sein, dann wird Ihnen die Software eine Nachricht mit dem Identifier des erforderlichen Bandes anzeigen. Laden Sie das Band und klicken Sie dann auf **Wiederholen**, um mit der Wiederherstellung fortzufahren.

7.4.4 Bandverwaltung

7.4.4.1 Erkennung von Bandgeräten

Beim Erkennen von Bandgeräten findet Acronis Backup & Recovery 11.5 an die Maschine angeschlossene Bandgeräte und schreibt die dazugehörigen Informationen in die Bandverwaltungsdatenbank. Das Erkennen von Bandgeräten ist notwendig:

- Nachdem Sie ein Bandgerät (erneut) angeschlossen haben.
- Nachdem Sie Acronis Backup & Recovery 11.5 (erneut) auf einer Maschine installiert haben, an die ein Bandgerät angeschlossen ist.

Beim Erkennen von Bandgeräten deaktiviert Acronis Backup & Recovery 11.5 diese im RSM.

So lassen Sie Bandgeräte erkennen

1. Klicken Sie im Verzeichnisbaum **Navigation** auf den Befehl **Bandverwaltung**. Wählen Sie, falls Sie mit dem Management Server verbunden sind, den Storage Node, an den Ihr Bandgerät angeschlossen ist.
2. Klicken Sie auf **Bandgeräte erkennen**. Sie sehen die Anzahl angeschlossener Bandgeräte, deren Laufwerke und Schächte.

7.4.4.2 Band-Pools

Acronis Backup & Recovery 11.5 verwendet so genannte Band-Pools, bei denen es sich um logische Gruppen von Bändern handelt. Die Software enthält bereits folgende vordefinierte Band-Pools: **Unbekannte Bänder**, **Importierte Bänder**, **Freie Bänder** und **Acronis**. Sie können außerdem auch Ihre eigenen, benutzerdefinierten Pools erstellen.

Vordefinierte Pools

Unbekannte Bänder

Der Pool enthält Bänder, die durch Anwendungen von Drittherstellern beschrieben wurden. Um auf diese Bänder schreiben zu können, müssen sie von Ihnen explizit in den Pool **Freie Bänder** verschoben (S. 236) werden. Sie können Bändern von diesem Pool zu keinem anderen Pool verschieben – mit Ausnahme des Pools **Freie Bänder**.

Importierte Bänder

Der Pool enthält Bänder, die von Acronis Backup & Recovery 11.5 in einem Bandgerät beschrieben wurden, das aber an einen anderen Storage Node oder Agenten angeschlossen war. Um auf diese Bänder schreiben zu können, müssen sie von Ihnen explizit in den Pool **Freie Bänder** verschoben werden. Sie können Bändern von diesem Pool zu keinem anderen Pool verschieben – mit Ausnahme des Pools **Freie Bänder**.

Freie Bänder

Der Pool enthält freie (leere) Bänder. Sie können Bänder von anderen Pools manuell zu diesem Pool verschieben.

Wenn Sie ein Band zum Pool **Freie Bänder** verschieben, kennzeichnet die Software diese als leer. Sollte das Band noch Backups enthalten, so werden diese als gelöscht angezeigt . Indem die Software die Backups überschreibt, entfernt sie auch alle mit diesen Backups verbundenen Daten aus der Datenbank.

Acronis

Der Pool wird standardmäßig für Backups verwendet, wenn Sie keine eigenen Pools erstellen wollen. Das trifft üblicherweise bei Bandlaufwerken mit einer kleinen Zahl von Bändern zu.

Benutzerdefinierte Pools

Sie müssen mehrere Pools erstellen, falls Sie Backups mit unterschiedlichen Daten separieren wollen. Sie können benutzerdefinierte Pools beispielsweise erstellen, um folgende Daten zu trennen:

- Backups aus unterschiedlichen Abteilungen Ihrer Firma
- Backups von verschiedenen Maschinen
- Backups von System-Volumes und Benutzerdaten
- befüllte Bänder von Bändern, auf die noch geschrieben wird (S. 234).

Befüllte Bänder trennen

Sie möchten möglicherweise bereits befüllte Bänder von solchen trennen, die noch unvollständig beschrieben sind. Angenommen, Sie wollen, dass Bänder, die über einen Monat mit Daten befüllt wurden, zu einem externen Aufbewahrungsort überführt werden. So gehen Sie dafür vor:

1. Erstellen Sie einen benutzerdefinierten Band-Pool (S. 234) (beispielsweise **Befüllte Bänder**).
2. Erstellen Sie einen anderen benutzerdefinierten Band-Pool (beispielsweise **Aktuelle Bänder**). Aktivieren Sie in den Pool-Einstellungen das Kontrollkästchen **Wenn Band voll ist, verschiebe zu Pool** und wählen Sie den Pool **Befüllte Bänder** aus der Liste.
3. Erstellen Sie ein Depot (S. 242) und assoziieren Sie es mit dem Pool **Aktuelle Bänder**.
4. Wählen Sie bei Erstellung eines Backup-Plans das erstellte Depot als den Backup-Zielort.
5. Werfen Sie einmal im Monat die Bänder des Pools **Befüllte Bänder** aus, und überführen Sie diese zu einem externen Aufbewahrungsort.

7.4.4.3 Aktionen mit Pools

Einen Pool erstellen

So erstellen Sie einen Pool:

1. Klicken Sie im Verzeichnisbaum **Navigation** auf den Befehl **Bandverwaltung**. Wählen Sie, falls Sie mit dem Management Server verbunden sind, den Storage Node, an den Ihr Bandgerät angeschlossen ist.
2. Klicken Sie auf **Pool erstellen**.
3. Spezifizieren Sie den Pool-Namen.
4. [Optional] Wählen Sie Bänder, die zu diesem Pool vom Pool **Freie Bänder** verschoben werden sollen.
5. [Optional] Deaktivieren Sie das '**Bänder automatisch vom Pool 'Freie Bänder' nehmen...**'-Kontollkästchen. Wenn es deaktiviert ist, werden nur solche Bänder für Backups verwendet, die zu einem bestimmten Moment in den neuen Pool aufgenommen wurden.
6. [Optional] Aktivieren Sie das Kontrollkästchen **Nach... Überschreibungen, Band verschieben zu Pool**, spezifizieren Sie dann die Anzahl an Informationsschreibzyklen und wählen Sie dann den Pool, zu dem ein Band anschließend verschoben wird.

   Tipp: Bändern haben eine relativ begrenzte Haltbarkeit. Sie können daher einen speziellen Pool erstellen und alte Bänder zu diesem verschieben lassen. Dadurch können Sie in diesem Pool gespeicherte Bänder regelmäßig auswerfen lassen, sie entsorgen und Ihr Bandgerät mit neuen Bändern beladen.

7. [Optional] Aktivieren Sie das Kontrollkästchen **Nach... Backups, Band verschieben zu Pool**, spezifizieren Sie dann die Anzahl an Backups und wählen Sie dann den Pool, zu dem ein Band anschließend verschoben wird.

   Tipp: Diese Option kann beispielsweise in folgenden Fällen nützlich sein: Sie sichern Ihre Maschine einmal täglich von Montag bis Freitag und verschieben das Band/die Bänder nach fünf Backups zum benutzerdefinierten Pool. Einmal wöchentlich entnehmen spezielle Mitarbeiter die Bänder aus diesem Pool und überführen Sie zu einer sicheren, externen Aufbewahrungsort.
8. [Optional] Aktivieren Sie das Kontrollkästchen **Wenn Band voll ist, verschiebe zu Pool** und wählen Sie dann den Pool, zu dem ein Band verschoben wird, wenn es voll ist.

   Tipp: Diese Option kann beispielsweise nützlich sein, um befыllte Bдnder von Bдndern zu trennen, auf die noch geschrieben wird (S. 234).
9. Klicken Sie auf **OK**.

Einen Pool bearbeiten

Sie können die Parameter des Pools **Acronis** oder Ihres eigenen, benutzerdefinierten Pools bearbeiten.

So bearbeiten Sie einen Pool:

1. Klicken Sie im Verzeichnisbaum **Navigation** auf den Befehl **Bandverwaltung**. Wählen Sie, falls Sie mit dem Management Server verbunden sind, den Storage Node, an den Ihr Bandgerät angeschlossen ist.
2. Wählen Sie den gewünschten Pool und klicken Sie dann auf **Einstellungen**.
3. Sie können den Pool-Namen ändern (ausgenommen den Namen des Pools **Acronis**) oder andere Einstellungen vornehmen. Zu weiteren Informationen über Pool-Einstellungen siehe den Abschnitt 'Einen Pool erstellen (S. 234)'.
4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Einen Pool löschen

Sie können nur benutzerdefinierte Pools löschen. Vordefinierte Band-Pools (**Unbekannte Bänder**, **Importierte Bänder**, **Freie Bänder** und der Pool **Acronis**) können nicht gelöscht werden.

So löschen Sie einen Pool:

1. Klicken Sie im Verzeichnisbaum **Navigation** auf den Befehl **Bandverwaltung**. Wählen Sie, falls Sie mit dem Management Server verbunden sind, den Storage Node, an den Ihr Bandgerät angeschlossen ist.
2. Wählen Sie den benötigten Pool und klicken Sie dann auf **Entfernen**.
3. Sollte der Pool mit einem oder mehreren Depots assoziiert sein, dann werden Sie vom System benachrichtigt, dass der Pool nicht gelöscht werden kann. Sie müssen auf **Schließen** klicken, den Pool in den Einstellungen eines jeden Depots ändern, welches in der Benachrichtigungsmeldung genannt wurde – und dann die Aktion zum Löschen des Pools wiederholen.

   Wählen Sie anderenfalls den Pool, zu dem die Bänder des zu löschenden Pools nach seiner Entfernung verschoben werden sollen.
4. Klicken Sie auf **OK**, um den Pool zu löschen.

7.4.4.4 Aktionen mit Bändern

Umbenennung

Falls die Software ein neues Band ermittelt, weist sie diesem automatisch einen Namen in folgendem Format zu: **Band XXX**, wobei **XXX** eine eindeutige Nummer ist. Bändern werden fortlaufend nummeriert. Die Umbenennungsaktion ermöglicht Ihnen, den Namen eines oder mehrerer Bänder manuell zu ändern.

So benennen Sie Bänder um:

1. Klicken Sie im Verzeichnisbaum **Navigation** auf den Befehl **Bandverwaltung**. Wählen Sie, falls Sie mit dem Management Server verbunden sind, den Storage Node, an den Ihr Bandgerät angeschlossen ist.
2. Klicken Sie auf den Pool, der das gewünschte Band (Bänder) enthält, und wählen Sie dann das erforderliche Band (Bänder).
3. Klicken Sie auf **Umbenennen**.
4. Geben Sie (einen) neue(n) Namen für das gewählte Band (die Bänder) ein.
5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Den Pool ändern

Diese Aktion ermöglicht Ihnen, ein Band oder mehrere Bänder von einem Pool zu einem anderen zu verschieben.

Wenn Sie ein Band zum Pool **Freie Bänder** verschieben, kennzeichnet die Software diese als leer. Falls das Band Backups enthält, so sind diese mit dem Symbol gekennzeichnet. Wenn die Software mit dem Überschreiben des Bandes beginnt, werden die mit den Backups verbundenen Daten aus der Datenbank entfernt.

Anmerkungen zu besonderen Bandtypen

- Sie können keine schreibgeschützten Bänder und keine einmal beschreibbaren WORM-Bänder (Write-Once-Read-Many) in den Pool **Freie Bänder** verschieben.
- Reinigungsbänder werden immer im Pool **Unbekannte Bänder** angezeigt; diese können von Ihnen zu keinem anderen Pool verschoben werden.

So verschieben Sie Bänder zu einem anderen Pool:

1. Klicken Sie im Verzeichnisbaum **Navigation** auf den Befehl **Bandverwaltung**. Wählen Sie, falls Sie mit dem Management Server verbunden sind, den Storage Node, an den Ihr Bandgerät angeschlossen ist.
2. Klicken Sie auf den Pool, der die notwendigen Bänder enthält und wählen Sie dann die benötigten Bänder.
3. Klicken Sie auf **Pool ändern**.
4. [Optional] Klicken Sie auf **Pool erstellen**, falls Sie für die gewählten Bänder einen anderen Pool erstellen wollen. Führen Sie die im Abschnitt „Einen Pool erstellen“ (S. 234) beschriebenen Aktionen aus.
5. Wählen Sie den Pool, zu dem die Bänder verschoben werden sollen.
6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Zu einem anderen Schacht verschieben

Verwenden Sie die Aktion in folgenden Situationen:

- Sie müssen mehrere Bänder gleichzeitig aus einem Bandgerät herausnehmen.
- Ihr Bandgerät hat keinen 'Mail-Schacht' und die herauszunehmenden Bänder befinden sich in Schächten von fest angeschlossenen Magazinen.

Sie müssen Bänder zu den Schächten von Ein-Schacht-Magazinen verschieben und das Magazin dann manuell herausnehmen.

So verschieben Sie Bänder zu anderen Schächten:

1. Klicken Sie im Verzeichnisbaum **Navigation** auf den Befehl **Bandverwaltung**. Wählen Sie, falls Sie mit dem Management Server verbunden sind, den Storage Node, an den Ihr Bandgerät angeschlossen ist.
2. Klicken Sie auf den Pool, der die notwendigen Bänder enthält und wählen Sie dann die benötigten Bänder.
3. Klicken Sie auf **Verschieben**.
4. Wählen Sie einen neuen Schacht, zu dem jedes der gewählten Bänder verschoben werden soll.
5. Klicken Sie auf **OK**, um die Aktion zu starten.

Auswerfen

Zum erfolgreichen Auswerfen eines Bandes aus einer Bandbibliothek muss diese den 'Mail-Schacht' haben und dieser darf nicht durch einen Benutzer oder eine andere Software gesperrt sein.

So lassen Sie ein Band auswerfen:

1. Klicken Sie im Verzeichnisbaum **Navigation** auf den Befehl **Bandverwaltung**. Wählen Sie, falls Sie mit dem Management Server verbunden sind, den Storage Node, an den Ihr Bandgerät angeschlossen ist.
2. Klicken Sie auf den Pool, der das gewünschte Band enthält, und wählen Sie dann das erforderliche Band.
3. Klicken Sie auf **Auswerfen**. Die Software fordert Sie auf, die Bandbeschreibung bereitzustellen. Wir empfehlen, dass Sie den physikalischen Speicherort beschreiben, wo das Band aufbewahrt wird. Die Software zeigt während einer Wiederherstellung diese Beschreibung an, so dass Sie das Band einfach finden können.

   Details. Sie können die Abfrage der Bandbeschreibung deaktivieren, indem Sie auf **Diese Meldung nicht wieder anzeigen** klicken. So reaktivieren Sie die Eingabeaufforderung: klicken Sie im Menü auf **Optionen**, dann auf **Konsolen-Optionen**, dann auf **Pop-up-Meldungen** und aktivieren Sie anschließend das Kontrollkästchen **Erfrage Beschreibung bei Auswurf des Bandes**.
4. Klicken Sie auf **OK**, um die Aktion zu starten.

Nachdem ein Band manuell oder automatisch (S. 138) ausgeworfen wurde, empfiehlt es sich, den entsprechenden Namen auf das Band zu schreiben.

Löschen

Wird ein Band physikalisch gelöscht, so werden auch alle auf dem Band gespeicherten Backups gelöscht und die dazugehörigen Informationen aus der Datenbank. Die Information über das Band selbst verbleibt jedoch in der Datenbank.

Nach dem Löschen wird ein Band, das sich im Pool **Unbekannte Bänder** oder **Importierte Bänder** befand, in den Pool **Freie Bänder** verschoben. Ein in einem anderen Pool befindliches Band wird nicht verschoben.

Sie können diese Aktion mit nur je einem Band gleichzeitig durchführen.

So löschen Sie ein Band:

1. Klicken Sie im Verzeichnisbaum **Navigation** auf den Befehl **Bandverwaltung**. Wählen Sie, falls Sie mit dem Management Server verbunden sind, den Storage Node, an den Ihr Bandgerät angeschlossen ist.
2. Klicken Sie auf den Pool, der das gewünschte Band enthält, und wählen Sie dann das erforderliche Band.
3. Klicken Sie auf **Löschen**. Das System erfragt eine Bestätigung der Aktion.
4. Klicken Sie auf **OK**, um die Aktion zu starten.

   Details: Sie können die Lösch-Aktion nicht abbrechen.

Erneut scannen

Die Informationen über den Inhalt der Bänder werden in einer dedizierten Datenbank gespeichert. Die Aktion 'Erneut scannen' liest den Inhalt der Bänder ein und aktualisiert die Datenbank, falls die dort befindlichen Informationen nicht mit den auf den Bändern gespeicherten Daten übereinstimmen. Die als Folge der Aktion ermittelten Archive werden in dem spezifizierten Depot platziert.

Sie können innerhalb einer Aktion die Bänder eines Pools erneut scannen lassen. Nur 'online' Bänder können für die Aktion ausgewählt werden.

Führen Sie 'Erneut scannen' aus:

- Falls die Datenbank eines Storages Nodes oder einer verwalteten Maschine verloren ging oder beschädigt wurde.
- Falls die Informationen über ein Band in der Datenbank nicht mehr aktuell sind (beispielsweise, weil der Inhalt eines Bandes durch einen anderen Storage Node oder Agenten modifiziert wurde).
- Um auf die auf Bändern gespeicherten Backups zugreifen zu können, wenn Sie unter einem bootfähigen Medium arbeiten.
- Falls Sie die Informationen über ein Band versehentlich von der Datenbank entfernt (S. 241) haben. Wenn Sie ein zuvor entferntes Band erneut scannen, erscheinen die auf diesem gespeicherten Backups erneut in der Datenbank und werden für Recovery-Aktionen verfügbar.
- Falls Backups von einem Band entweder manuell oder durch Aufbewahrungsregeln (S. 485) gelöscht wurden, Sie diese aber wieder für Recovery-Aktionen verfügbar haben wollen. Bevor Sie ein solches Band erneut scannen, sollten Sie es zuerst auswerfen (S. 237), seine Information aus der Datenbank entfernen (S. 241) und das Band danach wieder in das Bandgerät einlegen.

So scannen Sie Bänder neu:

1. Falls Sie noch kein bandbasiertes Depot (S. 242) mit dem Gerät assoziiert haben, in das Sie die Bänder geladen haben, dann erstellen Sie ein solches Depot.
2. Klicken Sie im Verzeichnisbaum **Navigation** auf den Befehl **Bandverwaltung**. Wählen Sie, falls Sie mit dem Management Server verbunden sind, den Storage Node, an den Ihr Bandgerät angeschlossen ist.
3. Führen Sie eine schnelle Inventarisierung (S. 239) durch.

Hinweis: *Aktivieren Sie während der Inventarisierung* nicht *das Kontrollkästchen* ***Neu erkannte Bänder vom Pool 'Unbekannte Bänder' oder 'Importierte Bänder' zum Pool 'Freie Bänder' verschieben****.*

4. Klicken Sie auf **Erneut scannen**.
5. Bestimmen Sie das Depot, in dem die neu ermittelten Archive abgelegt werden.
6. Wählen Sie den Pool **Unbekannte Bänder**. Das ist der Pool, zu dem die Mehrheit der Bänder als Ergebnis einer schnellen Inventarisierung gesendet wird. Ein erneutes Scannen des mit dem gewählten Depot assoziierten Pools oder des Pools **Importierte Bänder** ist auch möglich.
7. Wählen Sie die erneut zu scannenden Bänder. Aktivieren Sie zur Wahl aller Bänder des Pools das Kontrollkästchen neben dem Spaltenkopf **Bandname**.
8. Aktivieren Sie bei Bedarf das Kontrollkästchen **Datei-Recovery für auf Bändern gespeicherte Laufwerk-Backups aktivieren**.

   Details: Falls das Kontrollkästchen aktiviert ist, erstellte die Software zusätzliche Dateien auf einem Festplattenlaufwerk der Maschine, an welche das Bandgerät angeschlossen ist. Datei-Recovery von Laufwerk-Backups ist möglich, solange diese zusätzlichen Dateien intakt sind. Stellen Sie sicher, dass das Kontrollkästchen aktiviert ist, falls die Bänder Single-Pass-Backups (S. 494) enthalten. Anderenfalls werden Sie nicht in der Lage sein, Applikationsdaten von diesen Backups wiederherzustellen.
9. Sollten die Bänder ein kennwortgeschütztes Archiv enthalten, dann aktivieren Sie das entsprechende Kontrollkästchen und spezifizieren Sie das Kennwort des Archivs im Feld **Kennwort**. Ohne oder bei falscher Angabe des Kennwortes werden die Archive nicht erkannt. Beachten Sie dies, falls Sie nach dem erneuten Scannen keine Archive sehen.

   Tipp: Sollten die Bänder mehrere kennwortgeschützte Archive enthalten, die wiederum verschiedene Kennwörter verwenden, dann müssen Sie das erneute Scannen mehrfach wiederholen, um jedes Kennwort entsprechend einzugeben.
10. Klicken Sie auf **Start**, damit das erneute Scannen beginnt.

Ergebnis: Die gewählten Bänder werden zu dem mit dem gewählten Depot assoziierten Pool verschoben. Die auf diesen Bändern gespeicherten Backups können in diesem Depot gefunden werden. Ein über mehrere Bänder verteiltes Backup erscheint solange nicht im Depot, bis alle entsprechenden Bänder erneut gescannt wurden.

Inventarisierung

Die Inventarisierungsaktion ermittelt in ein Bandgerät geladene Bänder und weist denjenigen Bändern Namen zu, die keine haben. Führen Sie diesen Aktion jedes Mal aus, wenn Sie Bänder in die Kassettenschächte des Bandgerätes laden.

Inventarisierungsmethoden

Acronis Backup & Recovery 11.5 stellt die folgenden zwei Methoden zur Inventarisierung bereit.

Schnelle Inventarisierung

Acronis Backup & Recovery 11.5 scannt Bänder nach Barcodes. Durch die Verwendung von Barcodes kann die Software ein Band schnell zu dem Pool zurückgeben, wo es zuvor vorlag.

Verwenden Sie diese Methode, um Bänder zu erkennen, die von demselben und an dieselbe Maschine angeschlossenen Bandgerät verwendet wurden. Andere Bänder werden an den Pool **Unbekannt Bänder** gesendet.

Sollte Ihre Bandbibliothek keinen Barcode-Leser enthalten, dann werden alle Bänder an den Pool **Unbekannte Bänder** gesendet. Führen Sie zur Erkennung Ihrer Bänder eine vollständige

Inventarisierung durch – oder kombinieren Sie (wie weiter unten beschrieben) eine schnelle und eine vollständige Inventarisierung.

Vollständige Inventarisierung

Acronis Backup & Recovery 11.5 liest durch Acronis-Software geschriebene Tags und analysiert weitere Informationen über den Inhalt der geladenen Bänder. Verwenden Sie diese Methode, um leere Bänder zu erkennen – sowie Bänder, die durch Acronis-Software auf beliebigen Bandgeräten und Maschinen beschrieben wurden.

Die nachfolgende Tabelle zeigt Pools an, zu denen Bänder als Ergebnis der vollständigen Inventarisierung gesendet werden.

Band wurde verwendet von...	Band wird gelesen von...	Band wird gesendet zu Pool...
Agent	derselbe Agent	wo das Band zuvor war
	ein anderer Agent	**Importierte Bänder**
	Storage Node	**Importierte Bänder**
Storage Node	derselbe Storage Node	wo das Band zuvor war
	ein anderer Storage Node	**Importierte Bänder**
	Agent	**Importierte Bänder**
Dritthersteller-Backup-Anwendung	Agent oder Storage Node	**Unbekannte Bänder**

Bänder bestimmter Typen werden zu besonderen Pools gesendet:

Bandtyp	Band wird gesendet zu Pool...
Leere Bänder	**Freie Bänder**
Leeres, schreibgeschütztes Band	**Unbekannte Bänder**
Reinigungsband	**Unbekannte Bänder**

Die schnelle Inventarisierung kann auf komplette Bandgeräte angewendet werden. Die vollständige Inventarisierung kann auf komplette Bandgeräte, individuelle Laufwerke oder Schächte angewendet werden.

Schnelle und vollständige Inventarisierung kombinieren

Die vollständige Inventarisierung eines kompletten Bandgerätes kann viel Zeit benötigen. Sollten Sie nur einige wenige Bänder inventarisieren müssen, dann können Sie folgendermaßen vorgehen:

1. Führen Sie eine schnelle Inventarisierung des Bandgerätes durch.
2. Klicken Sie auf den Pool **Unbekannte Bänder**. Ermitteln Sie die Bänder, die Sie inventarisieren wollen, und notieren Sie sich die Schächte, die diese Bänder belegen.
3. Führen Sie für diese Schächte eine vollständige Inventarisierung durch.

Aktionen nach der Inventarisierung

Falls Sie Backups auf Bänder durchführen wollen, die in den Pools **Unbekannte Bänder** oder **Importierte Bänder** vorliegen, dann verschieben (S. 236) Sie diese in den Pool **Freie Bänder** und dann zum Pool **Acronis** oder einen benutzerdefinierten Pool. Falls der Pool, zu dem die Backups erfolgen sollen, vom Typ wiederauffüllbar (S. 497) ist, können Sie die Bänder im Pool **Freie Bänder** belassen.

Falls Sie eine Wiederherstellung von einem Band ausführen wollen, das im Pool **Unbekannte Bänder** oder **Importierte Bänder** vorliegt, so müssen Sie es erneut scannen (S. 238). Das Band wird zu dem

Pool verschoben, der mit dem Depot verbunden ist, das Sie beim erneuten Scannen gewählt haben und die auf dem Band gespeicherten Backups erscheinen in diesem Depot.

Abfolge der Aktionen

1. Klicken Sie im Verzeichnisbaum **Navigation** auf den Befehl **Bandverwaltung**. Wählen Sie, falls Sie mit dem Management Server verbunden sind, den Storage Node, an den Ihr Bandgerät angeschlossen ist.
2. Klicken Sie auf **Bestandsliste** (Inventory).
3. Wählen Sie die Inventarisierungsmethode: **Schnell** oder **Vollständig**.
4. [Optional] Aktivieren Sie das Kontrollkästchen **Neu erkannte Bänder vom Pool 'Unbekannte Bänder' oder 'Importierte Bänder' zum Pool 'Freie Bänder' verschieben**.

   Warnung: *Aktivieren Sie dieses Kontrollkästchen nur, wenn Sie absolut sicher sind, dass die auf Ihren Bändern gespeicherten Daten überschrieben werden können.*

5. [Optional] Wählen Sie die zu inventarisierenden Bandbibliotheken und autonomen Laufwerke. Standardmäßig sind alle Bandbibliotheken und autonomen Laufwerke vorausgewählt.
6. [Optional] Falls Sie die **vollständige** Inventarisierungsmethode wählen, können Sie die zu inventarisierenden Bandbibliotheksschächte und Laufwerke bestimmen. Standardmäßig sind alle Schächte und Laufwerke vorausgewählt.

Entfernen

Durch die Aktion 'Entfernen' werden die Informationen über die auf dem gewählten Band gespeicherten Backups sowie die Informationen über das Band selbst aus der Datenbank gelöscht.

Sie können nur ein offline (ausgeworfenes (S. 237)) Band entfernen.

So entfernen Sie ein Band:

1. Klicken Sie im Verzeichnisbaum **Navigation** auf den Befehl **Bandverwaltung**. Wählen Sie, falls Sie mit dem Management Server verbunden sind, den Storage Node, an den Ihr Bandgerät angeschlossen ist.
2. Klicken Sie auf den Pool, der das gewünschte Band enthält, und wählen Sie dann das erforderliche Band.
3. Klicken Sie auf **Entfernen**. Das System erfragt eine Bestätigung der Aktion.
4. Klicken Sie auf **OK**, um das Band zu entfernen.

Was sollen Sie tun, wenn Sie ein Band versehentlich entfernt haben?

Anders als bei einem gelöschten (S. 237) Band wurden die Daten eines entfernten Bandes nicht physikalisch gelöscht. Sie können daher die auf einem solchen Band gespeicherten Backups wieder verfügbar machen. Gehen Sie folgendermaßen vor:

1. Laden Sie das Band in Ihr Bandgerät.
2. Führen Sie eine schnelle Inventarisierung (S. 239) durch, um das Band erkennen zu lassen.

   Aktivieren Sie während der Inventarisierung nicht *das Kontrollkästchen* ***Neu erkannte Bänder vom Pool 'Unbekannte Bänder' oder 'Importierte Bänder' zum Pool 'Freie Bänder' verschieben****.*

3. Führen Sie die Aktion 'Erneut scannen (S. 238)' durch, um die auf den Bändern gespeicherten Daten mit der Datenbank abzugleichen.

7.4.5 Depots auf Bändern

Jedes bandbasierte Depot ist mit einem oder mehreren Laufwerken eines Bandgerätes sowie einem Pool (S. 233) von Bändern assoziiert.

Warum benötigte ich mehrere Depots?

Zwei der häufigsten Szenarien, die es erforderlich machen, dass Sie mehrere Depots erstellen, sind wie folgt:

- Sie möchten die Daten mehrerer Maschinen so sichern, dass sich die Backups von jeder Maschine auf einem separaten Bandsatz befinden.
- Sie möchten unterschiedliche Daten derselben Maschine auf separate Bandsätze sichern. Beispielsweise soll das System-Volume wöchentlich gesichert werden, sich häufig ändernde Daten dagegen täglich.

In beiden Fällen erstellen Sie einen separaten, benutzerdefinierten Pool für jeden Bandsatz und assoziieren ein separates Depot mit diesem.

Persönliche, bandbasierte Depots

Bevor Sie eine Maschine auf ein direkt angeschlossenes Bandgerät sichern, können Sie ein persönliches Depot erstellen. Falls Sie das nicht wollen, dann wird die Software automatisch ein persönliches Depot erstellen, welches mit dem Pool **Acronis** assoziiert ist.

Sollten Sie mehr als ein persönliches Depot erstellen, dann werden die Bänder mit Backups gemäß den Einstellungen dieser Depots in die entsprechenden Pools platziert. Jedes Depot zeigt jedoch alle Backups an, die in all diesen Depots hinterlegt sind.

So erstellen Sie ein persönliches Depot:

1. Klicken Sie im Verzeichnisbaum **Navigation** auf **Depots**.
2. Klicken Sie auf **Erstellen**.
3. Fahren Sie fort, wie im Abschnitt 'Ein persönliches Depot erstellen (S. 215)' beschrieben.

Verwaltete, zentrale, bandbasierte Depots

Um eine Maschine auf ein an einem Storage Node angeschlossenen Bandgerät zu sichern, müssen Sie ein verwaltetes, zentrales Depot auf dem Bandgerät erstellen.

So erstellen Sie ein verwaltetes, zentrales Depot:

1. Klicken Sie im Verzeichnisbaum **Navigation** auf **Storage Nodes**.
2. Wählen Sie den benötigten Storage Node und klicken Sie dann auf **Depot erstellen**.
3. Fahren Sie fort wie im Abschnitt 'Ein verwaltetes zentrales Depot erstellen (S. 206)' beschrieben.

Tipp: Falls Sie mehrere Maschinen zu einer Bandbibliothek mit multiplen Laufwerken sichern, dann assoziieren Sie das Depot mit der kompletten Bibliothek. Das ermöglicht Ihnen, die Backups der Maschinen simultan über verschiedene Laufwerke durchzuführen. Falls Sie ein Depot oder mehrere Depots mit nur einem Laufwerk assoziieren, werden die Laufwerke in eine Warteschlange gestellt.

7.4.6 Anwendungsbeispiele

Neben den in diesem Abschnitt bereits beschriebenen Beispielen können Sie noch zwei weitere Beispiele berücksichtigen:

- Verschieben älterer Backups auf Bänder zur Langzeitaufbewahrung (S. 112) (Laufwerk-zu-Laufwerk-zu-Band)

- Backup auf Bänder innerhalb eines engen Backup-Fensters (S. 112)

7.4.6.1 Beispiel 1: Ein Band-Autoloader und 12 Bänder

Betrachten Sie folgendes Szenario:

- Sie haben 12 Bänder und einen Band-Autoloader an die Maschine angeschlossen, deren Daten Sie per Backup sichern wollen.
- Sie möchten die Daten der Maschine so sichern, dass das Backup auf einem anderen Band fortgesetzt wird, falls auf dem ursprünglichen Band kein ausreichender Speicherplatz vorhanden ist.
- Wenn alle Bänder befüllt sind, sollen sie nacheinander wieder – ohne Benutzereingriff – überschrieben werden.

Sie benötigen einen separaten Pool für den Backup-Plan, der dieses Szenario ausführt. Falls Sie andere Backup-Pläne haben oder erstellen wollen, die auf dasselbe Bandgerät schreiben, dann verwenden Sie für diese Pläne andere Pools.

Abfolge der Aktionen

1. Laden Sie Ihre Bänder in die Autoloader-Schächte.
2. Führen Sie die Inventarisierung (S. 239) mit aktiviertem Kontrollkästchen **Neu erkannte Bänder vom Pool 'Unbekannte Bänder' oder 'Importierte Bänder' zum Pool 'Freie Bänder' verschieben** durch.

   Ergebnis. Die geladenen Bänder befinden sich im Pool **Freie Bänder**. Falls einige davon an den Pool **Acronis** oder einen benutzerdefinierten Pool gesendet werden, dann bedeutet dies, dass diese Bänder Backups enthalten, die Sie früher auf dieser Maschine erstellt haben. Verschieben (S. 236) Sie solche Bänder manuell in den Pool **Freie Bänder**, falls Sie diese Backups nicht mehr benötigen.
3. Entscheiden Sie, ob Ihre Backups auf Bänder erfolgen sollen, die sich im vorgegebenen **Acronis**-Pool (S. 233) befinden – oder ob Sie einen neuen Pool erstellen (S. 234) wollen. Deaktivieren Sie in beiden Fällen in den Einstellungen des gewählten Pools das Kontrollkästchen **Bänder automatisch vom Pool 'Freie Bänder' nehmen...**.
4. Verschieben Sie alle geladenen Bänder vom Pool **Freie Bänder** zu dem von Ihnen gewählten Pool.
5. Erstellen Sie ein persönliches Depot (S. 242) und assoziieren Sie Ihren Pool mit diesem.
6. Bei Erstellung eines Backup-Plans (S. 58):
   - Wählen Sie Ihr Depot als den Backup-Speicherort.
   - Wählen Sie das Backup-Schema **Benutzerdefiniert**. Konfigurieren Sie die Backup-Planungen so, dass das komplette Set der 12 Bänder wenigstens 2 vollständige Backups enthält. Dadurch erhält die Software die Möglichkeit, Bänder gegebenenfalls zu überschreiben.
   - Wählen Sie bei **Archiv bereinigen** die Option **Wenn nicht ausreichend Speicherplatz während des Backups vorhanden ist**.

Ergebnis

Der Backup-Plan wird nur die Bänder verwenden, die sich in dem gewählten Pool befinden. Wenn alle Bänder vollgeschrieben sind, wird das älteste Band überschreiben – und so weiter.

7.4.6.2 Beispiel 2: Backups auf Bänder auf Basis einer wöchentlichen Rotation

Betrachten Sie folgendes Szenario:

- Sie möchten mehrere Maschinen auf ein Bandgerät sichern, das an einem Acronis Backup & Recovery 11.5 Storage Node angeschlossen ist.
- Sie möchten freitags ein Voll-Backup erstellen sowie inkrementelle Backups je am Montag, Dienstag, Mittwoch und Donnerstag.
- Sie möchten zwei Bandsätze verwenden, jeder davon soll über eine Woche beschrieben werden. Der Bandsatz einer gerade verstrichenen Woche soll ausgeworfen und durch den anderen Satz ersetzt werden, der dann später im Wechsel überschrieben werden soll. Dieser Arbeitsansatz kann nützlich sein, wenn die Anzahl der Schächte in Ihrem Bandgerät nur für die Backups je einer Woche ausreicht.

Abfolge der Aktionen

1. Laden Sie einen Ihrer Bandsätze in die Bandgerätschächte.
2. Führen Sie die Inventarisierung (S. 239) mit aktiviertem Kontrollkästchen **Neu erkannte Bänder vom Pool 'Unbekannte Bänder' oder 'Importierte Bänder' zum Pool 'Freie Bänder' verschieben** durch.

   Ergebnis. Die geladenen Bänder befinden sich im Pool **Freie Bänder**. Falls einige davon an den Pool **Acronis** oder einen benutzerdefinierten Pool gesendet werden, dann bedeutet dies, dass diese Bänder Backups enthalten, die Sie früher auf dieser Maschine erstellt haben. Verschieben (S. 236) Sie solche Bänder manuell in den Pool **Freie Bänder**, falls Sie diese Backups nicht mehr benötigen.
3. Entscheiden Sie, ob Ihre Backups auf Bänder erfolgen sollen, die sich im vorgegebenen **Acronis**-Pool (S. 233) befinden – oder ob Sie einen neuen Pool erstellen (S. 234) wollen.
4. Falls der gewählte Pool nicht wiederauffüllbar (S. 497) ist, dann verschieben Sie alle geladenen Bänder aus dem Pool **Freie Bänder** in den von Ihnen gewählten Pool.
5. Lassen Sie den geladenen Bandsatz auswerfen. Wiederholen Sie für den anderen Bandsatz die Schritte 1, 2 und 4.
6. Ein verwaltetes Depot erstellen (S. 206): Wenn Sie das Depot erstellen:
   - Wählen Sie bei **Laufwerke** das komplette Bandlaufwerk. Dadurch ermöglichen Sie gleichzeitige Backups der Maschinen mit Hilfe unterschiedlicher Laufwerke, sofern Ihr Bandgerät über mehr als ein Laufwerk verfügt.
   - Wählen Sie bei **Band-Pool** denjenigen Pool, wohin Sie Ihre Backups erstellen wollen (den Pool **Acronis** oder den neu erstellten).
7. Bei Erstellung eines zentralen Backup-Plans (S. 396):
   - Wählen Sie bei **Elemente für das Backup** die Maschinen, die Sie sichern wollen.
   - Wählen Sie das erstellte Depot als den Backup-Zielort.
   - Wählen Sie das Backup-Schema **Benutzerdefiniert**.
   - Spezifizieren Sie die Planungen für die vollständigen und inkrementellen Backups.
   - Wählen Sie bei **Archiv bereinigen** die Option **Aufbewahrungsregeln verwenden** und klicken Sie dann auf **Aufbewahrungsregeln**. Spezifizieren Sie die Aufbewahrungsregel so, dass Backups älter als 1 Woche gelöscht werden.
8. Lassen Sie jeden Freitag, bevor ein neues Voll-Backup ausgeführt wird, den geladenen Bandsatz auswerfen und legen Sie den anderen ein. Sollte Ihr Bandgerät einen Barcode-Leser enthalten,

dann führen Sie eine schnelle Inventarisierung aus. Führen Sie ansonsten eine vollständige Inventarisierung durch.

Ergebnis

Die Bandsätze werden abwechselnd verwendet. Wenn ein Bandsatz eingelegt wird, werden seine Bänder nacheinander überschrieben.

7.4.6.3 Beispiel 3: Laufwerk-zu-Laufwerk-zu-Band mit Übermittlung der Bänder zu einem externen Speicherort

Betrachten Sie folgendes Szenario:

- Sie möchten das Backup einer Maschine auf ein Festplattenlaufwerk erstellen und dann eine Replikation jedes Backups auf das lokal angeschlossene Bandgerät durchführen.
- Sie möchten, dass die Bänder mit jedem Backup ausgeworfen und dann an einen externen Aufbewahrungsort übermittelt werden.

Abfolge der Aktionen

1. Beladen Sie die Bandgeräteschächte mit Bändern.
2. Führen Sie die Inventarisierung (S. 239) mit aktiviertem Kontrollkästchen **Neu erkannte Bänder vom Pool 'Unbekannte Bänder' oder 'Importierte Bänder' zum Pool 'Freie Bänder' verschieben** durch.

   Ergebnis: Die geladenen Bänder befinden sich im Pool **Freie Bänder**. Falls einige davon an den Pool **Acronis** oder einen benutzerdefinierten Pool gesendet werden, dann bedeutet dies, dass diese Bänder Backups enthalten, die Sie früher auf dieser Maschine erstellt haben. Verschieben (S. 236) Sie solche Bänder manuell in den Pool **Freie Bänder**, falls Sie diese Backups nicht mehr benötigen.
3. Entscheiden Sie, ob Ihre Backups auf Bänder erfolgen sollen, die sich im vorgegebenen **Acronis**-Pool (S. 233) befinden – oder ob Sie einen neuen Pool erstellen (S. 234) wollen.
4. Falls der gewählte Pool nicht wiederauffüllbar (S. 497) ist, dann verschieben Sie alle geladenen Bänder aus dem Pool **Freie Bänder** in den von Ihnen gewählten Pool.
5. Erstellen Sie ein persönliches Depot (S. 242) und assoziieren Sie Ihren Pool mit diesem.
6. Bei Erstellung eines Backup-Plans (S. 58):
   - Spezifizieren Sie einen lokalen Ordner als Backup-Zielort.
   - Legen Sie das benötigte Backup-Schema fest.
   - Aktivieren Sie das Kontrollkästchen **Neu erstelltes Backup zu einem anderen Speicherort replizieren**, klicken Sie auf **2. Speicherort** und wählen Sie das erstellte Depot aus dem Verzeichnisbaum.
   - Klicken Sie auf **Backup-Optionen**, dann im Verzeichnisbaum auf **Bandverwaltung** (S. 138) und aktivieren Sie das Kontrollkästchen **Bänder nach erfolgreichen Backups auswerfen**.
7. Nachdem ein Backup erstellt wurde und die entsprechenden Bänder ausgeworfen wurden, können Sie sie zu einem sicheren, externen Aufbewahrungsort übermitteln. Sollten Sie zur Fortführung der Backups nicht mehr genügend freie Bänder haben, dann laden Sie neue Bänder und führen Sie die Schritte 2 und 4 aus.

Ergebnis:

Die Backups der Maschine werden in dem lokalen Ordner und auf Bändern erstellt bzw. gespeichert. Die Bänder mit den jeweiligen Backups werden zum externen Aufbewahrungsort übermittelt.

7.4.6.4 Beispiel 4: GVS. Vollständige Backups zu einem externen (off-site) Storage senden

Betrachten Sie folgendes Szenario:

- Sie möchten die Backups einer Maschine auf ein Bandgerät erstellen lassen, das an einem Storage Node angeschlossen ist.
- Sie möchten das Großvater-Vater-Sohn-Backup-Schema verwenden (S. 70).
- Sie möchten vollständige, inkrementelle und differentielle Backups erstellen. Jedes vollständige Backup sollte auf ein separates Band geschrieben werden, damit Sie die Bänder mit den vollständigen Backups zu einem sicheren externen Aufbewahrungsort übertragen können.

Abfolge der Aktionen

1. Beladen Sie die Bandgeräteschächte mit Bändern.
2. Führen Sie die Inventarisierung (S. 239) mit aktiviertem Kontrollkästchen **Neu erkannte Bänder vom Pool 'Unbekannte Bänder' oder 'Importierte Bänder' zum Pool 'Freie Bänder' verschieben** durch.

   Ergebnis: Die geladenen Bänder befinden sich im Pool **Freie Bänder**. Falls einige davon an den Pool **Acronis** oder einen benutzerdefinierten Pool gesendet werden, dann bedeutet dies, dass diese Bänder Backups enthalten, die Sie früher auf dieser Maschine erstellt haben. Verschieben (S. 236) Sie solche Bänder manuell in den Pool **Freie Bänder**, falls Sie diese Backups nicht mehr benötigen.
3. Entscheiden Sie, ob Ihre Backups auf Bänder erfolgen sollen, die sich im vorgegebenen **Acronis**-Pool (S. 233) befinden – oder ob Sie einen neuen Pool erstellen (S. 234) wollen.
4. Falls der gewählte Pool nicht wiederauffüllbar (S. 497) ist, dann verschieben Sie alle geladenen Bänder aus dem Pool **Freie Bänder** in den von Ihnen gewählten Pool.
5. Ein verwaltetes Depot erstellen (S. 206): Wenn Sie das Depot erstellen:
   - Wählen Sie bei **Laufwerke** das komplette Bandlaufwerk. Dadurch ermöglichen Sie gleichzeitige Backups der Maschinen mit Hilfe unterschiedlicher Laufwerke, sofern Ihr Bandgerät über mehr als ein Laufwerk verfügt.
   - Wählen Sie bei **Band-Pool** denjenigen Pool, wohin Sie Ihre Backups erstellen wollen (den Pool **Acronis** oder den neu erstellten).
6. Bei Erstellung eines Backup-Plans (S. 58):
   - Wählen Sie das erstellte Depot als den Backup-Zielort.
   - Wählen Sie das Backup-Schema **Großvater-Vater-Sohn (GVS)**.
   - Spezifizieren Sie die Regeln so, dass tägliche Backups für 7 Tag bewahrt werden, wöchentliche für 4 Wochen und monatliche unbegrenzt.
   - Klicken Sie auf **Anzeigen: Backup-Typ, Validierung...** und wählen Sie dann bei **Backup-Typ** die Option **Vollständig/Inkrementell/Differentiell**.
   - Klicken Sie auf **Backup-Optionen**, dann im Verzeichnisbaum auf **Bandverwaltung** (S. 138) und wählen Sie die Option **Für jedes Voll-Backup** (under **Immer ein freies Band verwenden**).
7. Nachdem ein vollständiges Backup erstellt wurde, können Sie die entsprechenden Bänder auswerfen und zu einem sicheren externen Aufbewahrungsort übertragen. Sollten Sie zur Fortführung der Backups nicht mehr genügend freie Bänder haben, dann laden Sie neue Bänder und führen Sie die Schritte 2 und 4 aus.

Ergebnis:

Die Maschine wird in Übereinstimmung mit dem spezifizierten Backup-Schema auf die Bänder gesichert. Bänder mit vollständigen Backups werden zu einem sicheren externen Aufbewahrungsort gesendet.

7.5 Storage Node

Die folgenden Abschnitte beschrieben, wie Sie die Acronis Backup & Recovery 11.5 Storage Nodes verwenden.

Storage Nodes stehen nur in den Advanced-Editionen von Acronis Backup & Recovery 11.5 zur Verfügung.

7.5.1 Was ist ein Storage Node?

Der Acronis Backup & Recovery 11.5 Storage Node ist ein Server, der zur optimalen Nutzung verschiedener Ressourcen entwickelt wurde (z.B. unternehmensweite Speicherkapazität, Netzwerkbandbreite oder der CPU-Last verwalteter Maschinen), welche zum Schutz bzw. zur Sicherung von Unternehmensdaten erforderlich sind. Dieses Ziel wird durch Organisation und Verwaltung der Speicherorte erreicht, die als dedizierte Speicher für die Backup-Archive des Unternehmens (verwaltete Depots) dienen.

Die wichtigste Funktion eines Storage Nodes ist die Deduplizierung von Backups, die in seinen Depots gespeichert sind. Was bedeutet, dass identische Daten zu einem solchen Depot nur je einmal gesichert werden. Das reduziert die Netzwerkauslastung während der Backup-Erstellung sowie den durch die Archive belegten Speicherplatz.

Es können bis zu 50 Storage Nodes eingerichtet werden.

7.5.2 Unterstützte Storage-Typen

Ein verwaltetes Depot kann organisiert werden:

- Auf für den Storage Node lokal verfügbaren Festplatten
- Auf einer Netzwerkfreigabe
- Auf einem Storage Area Network (SAN)
- Auf einem Network Attached Storage-Gerät (NAS)
- Auf einer Bandbibliothek (S. 223), die lokal mit dem Storage Node verbunden ist.

7.5.3 Durch Storage Nodes durchgeführte Aktionen

Storage Nodes können folgende Aktionen mit in verwalteten Depots gespeicherten Archiven durchführen.

Bereinigung und Validierung

Archive, die in nicht verwalteten Depots gespeichert sind, werden durch die Agenten (S. 485) verwaltet, die die Archive erstellen. Das bedeutet, dass jeder Agent nicht nur Daten zu einem Archiv sichert, sondern auch Dienst-Tasks ausführt, die Aufbewahrungs- und Validierungsregeln auf das Archiv anwenden, wie sie im Backup-Plan (S. 486) spezifiziert wurden. Um die verwalteten Maschinen von unnötiger CPU-Last zu befreien, kann die Ausführung der Dienst-Tasks an den Storage Node delegiert werden. Da die Task-Planungen auf der Maschine vorliegen, auf der sich der Agent

befindet und da daher die Zeit bzw. die Ereignisse dieser Maschine verwendet werden, muss der Agent die Bereinigung und Validierung entsprechend der Planung auslösen. Dafür muss der Agent online sein. Die weitere Verarbeitung wird vom Storage Node übernommen.

Diese Funktionalität kann in einem verwalteten Depot nicht deaktiviert werden. Die nächsten beiden Aktionen sind optional.

Deduplizierung

Ein verwaltetes Depot kann als deduplizierendes Depot konfiguriert werden: Das bedeutet, dass identische Daten nur einmal zu diesem Depot gesichert werden, um die Netzwerkauslastung während der Backups sowie den durch die Archive belegten Speicherplatz zu minimieren. Zu weiteren Informationen siehe den Abschnitt 'Deduplizierung (S. 259)'.

Verschlüsselung

Ein verwaltetes Depot kann so konfiguriert werden, dass alle darauf geschriebenen Daten verschlüsselt und alle davon gelesenen Daten vom Storage Node wieder transparent entschlüsselt werden. Dazu wird ein für das Depot spezifischer Kodierungsschlüssel verwendet, der auf dem Server des Knotens gespeichert wird. Falls das Speichermedium gestohlen wird oder eine unbefugte Person darauf zugreift, wird der Übeltäter den Inhalt des Depots ohne Zugriff auf diesen speziellen Storage Node nicht entschlüsseln können.

Falls ein Archiv bereits durch einen Agenten verschlüsselt wurde, dann wendet der Storage Node seine eigene Verschlüsselung noch einmal über des Agenten an.

7.5.4 Erste Schritte mit einem Storage Node

Voraussetzungen

Stellen Sie sicher, dass:

- Der Management Server, die Konsole und die Agenten bereits installiert sind.
- Die Maschine, auf der der Storage Node installiert werden soll, den in der Installationsanleitung beschriebenen Systemanforderungen entspricht.
- Sie das Setup-Programm von Acronis Backup & Recovery 11.5 heruntergeladen haben.

Den Storage Node einrichten

1. Installieren Sie den Acronis Backup & Recovery 11.5 Storage Node.
    a. Melden Sie sich als Administrator an und starten Sie das Setup-Programm von Acronis Backup & Recovery 11.5.
    b. Klicken Sie auf **Acronis Backup & Recovery 11.5 installieren**.
    c. Nehmen Sie die Lizenzvereinbarung an.
    d. Aktivieren Sie das Kontrollkästchen **Backups anderer Maschinen auf dieser Maschine sichern**.
    e. Klicken Sie auf **Jetzt registrieren**. Geben Sie den Namen oder die IP-Adresse der Maschine an, auf der der Management Server installiert ist. Geben Sie den Benutzernamen und Kennwort eines Benutzers an, der Mitglied der Gruppe 'Acronis Centralized Admins' auf der Maschine des Management Servers ist.

        Details: Alternativ können Sie den Storage Node auch, wie in Schritt 2 beschrieben, zu einem späteren Zeitpunkt hinzufügen.
    f. Fahren Sie mit der Installation fort.

2. Fügen Sie den Storage Node dem Management Server hinzu. Überspringen Sie diesen Schritt, falls Sie den Storage Node bereits bei der Installation registriert haben.
   a. Verbinden Sie die Konsole mit dem Management Server und klicken Sie im Bereich **Navigation** auf **Storage Nodes**.
   b. Klicken Sie auf **Hinzufügen** und fahren Sie dann fort, wie im Abschnitt 'Einen Storage Node dem Management Server hinzufügen (S. 252)' beschrieben.
3. Erstellen Sie ein zentrales, verwaltetes Depot.
   a. Falls noch nicht verbunden, dann verbinden Sie die Konsole jetzt mit dem Management Server und klicken Sie dann im Bereich **Navigation** auf **Storage Nodes**.
   b. Wählen Sie den benötigten Storage Node und klicken Sie dann auf **Depot erstellen**. Die Seite **Zentrales Depot erstellen** wird mit dem vorausgewählten Storage Node geöffnet. Führen Sie dann die noch verbliebenen im Abschnitt 'Ein zentrales, verwaltetes Depot erstellen (S. 206)' beschriebenen Schritte zur Erstellung des Depots aus.

      Hinweis. Bedenken Sie bei Aktivierung der Deduplizierung für das Depot, dass das entsprechende Add-on zur Deduplizierung auf jeder Maschine vorhanden sein muss, die zu diesem Depot gesichert wird. Ohne dieses Add-on sind keine Backups zu einem deduplizierenden Depot möglich.

      Details: Folgen Sie den im Abschnitt 'Optimale Vorgehensweisen bei der Deduplizierung (S. 263)' gegebenen Empfehlungen, wenn Sie die Pfade zum Depot und der Deduplizierungsdatenbank spezifizieren.

Backup zum Storage Node

Erstellen Sie einen lokalen (S. 58) oder zentralen (S. 396) Backup-Plan. Spezifizieren Sie bei Erstellung des Backup-Plans das verwaltete Depot als Zielort zum Speichern der Backups.

Recovery von einem Storage Node

Folgen Sie den im Abschnitt 'Einen Recovery-Task erstellen (S. 146)' beschriebenen Schritten.

Storage Nodes verwalten

1. Verbinden Sie die Konsole mit dem Management Server.
2. Klicken Sie im Fensterbereich **Navigation** auf **Storage Nodes**.
3. Wählen Sie den Storage Node aus und führen Sie dann die gewünschten Aktionen durch, wie im Abschnitt 'Aktionen für Storage Nodes (S. 250)' beschrieben.

7.5.5 Benutzerberechtigungen auf einem Storage Node

Der Umfang an Berechtigungen, die Benutzer auf einem Acronis Backup & Recovery 11.5 Storage Node haben, kann unterschiedlich sein.

1. **Acronis Centralized Admins** – Administratoren des Management Servers, Mitglieder der Gruppe 'Acronis Centralized Admins'. Acronis Centralized Admins können:
   - Zentrale Depots erstellen, die vom Storage Node verwaltet werden sollen.
   - Konten für Depot-Administratoren und Depot-Benutzer hinzufügen, bearbeiten oder entfernen.
   - Jedes Archiv in jedem zentralen, durch den Storage Node verwalteten Depot einsehen und verwalten.
   - Indizierungen und Verdichtungen verwalten, wie im Abschnitt 'Aktionen für Storage Nodes (S. 250)' beschrieben.

2. **Depot-Administratoren** – eine Gruppe von Benutzerkonten auf dem Storage Node, die der Management Server-Administrator bei Erstellung oder Bearbeitung eines Depots auswählt. Depot-Administratoren können jedes Archiv in dem spezifizierten verwalteten Depot einsehen und verwalten. Standardmäßig wird die Gruppe 'Administratoren' des Storage Nodes den 'Depot-Administratoren' hinzugefügt.
3. **Depot-Benutzer** – eine Gruppe von Benutzerkonten auf dem Storage Node, die der Management Server-Administrator bei Erstellung oder Bearbeitung eines Depots auswählt. Depot-Benutzer können nur ihre eigenen im Depot gespeicherten Archive einsehen und verwalten. Standardmäßig wird die Gruppe 'Jeder' des Storage Nodes den 'Depot-Benutzern' hinzugefügt.

Empfehlungen zu Benutzerkonten

Damit Benutzer auf ein zentrales, durch den Storage Node verwaltetes Depot zugreifen können, müssen Sie sicherstellen, dass diese Benutzer auch die Berechtigung zum Zugriff auf den Storage Node über das Netzwerk haben.

Sind die Maschine des Benutzers und die des Storage Nodes gemeinsam in einer Active Directory-Domain, müssen Sie wahrscheinlich keine weiteren Schritte durchführen: alle Benutzer sind üblicherweise Mitglieder der Gruppe „Domain-Benutzer“ und können so auch auf den Storage Node zugreifen.

Anderenfalls müssen Sie auf der Maschine, auf der der Storage Node installiert ist, zusätzliche Benutzerkonten einrichten. Wir empfehlen, für jeden auf den Storage Node zugreifenden Benutzer ein separates Benutzerkonto zu erstellen, so dass die Benutzer nur auf die je ihnen gehörenden Archive zugreifen können.

Erweiterte Berechtigung für Maschinen-Administratoren

Ein Depot-Benutzer, der auf einer Maschine auch Mitglied der Gruppe 'Administratoren' ist, kann jedes Archiv, welches *von dieser Maschine* in einem verwalteten Depot erstellt wurde, einsehen und verwalten – ungeachtet welcher Art das Konto dieses Benutzers auf dem Storage Node ist.

Beispiel

Angenommen, zwei Benutzer auf einer Maschine, BenutzerA und BenutzerB, erstellen Backups von dieser Maschine – mit Hilfe eines Storage Nodes zu einem zentralen Depot. Fügen Sie diese Benutzer auf dem Storage Node als reguläre BenutzerA_SN bzw. BenutzerB_SN hinzu (nicht administrative Konten). Bei Erstellung eines verwalteten Depots wurden beide Konten als Depot-Benutzer hinzugefügt.

Normalerweise kann BenutzerA nur auf Archive zugreifen, die von BenutzerA erstellt wurden (und BenutzerA_SN gehören), was für BenutzerB entsprechend gilt (Zugriff nur auf von BenutzerB erstellte Archive, die BenutzerB_SN gehören).

Ist BenutzerA jedoch Mitglied der Gruppe Administratoren auf dieser Maschine, so kann er zusätzlich auf die Archive zugreifen, die von BenutzerB dieser Maschine erstellt wurden – und das obwohl das Konto von BenutzerA auf dem Storage Node ein reguläres ist.

7.5.6 Aktionen mit Storage Nodes

7.5.6.1 Aktionen für Storage Nodes

Zugriff auf Aktionen

1. Verbinden Sie die Konsole mit dem Management Server.

2. Klicken Sie im Fensterbereich **Navigation** auf **Storage Nodes**.
3. Die Aktionen werden durch Klicken auf die korrespondierenden Schaltflächen in der Symbolleiste ausgeführt.

Aufgabe	Lösung
Dem Management Server einen Storage Node hinzufügen	1. Klicken Sie auf **Hinzufügen**. 2. Geben Sie im Fenster **Storage Node hinzufügen** (S. 252) die Maschine an, auf der der Storage Node installiert ist. Wenn ein Storage Node hinzugefügt wird, wird eine Vertrauensstellung (Trusted Relationship) zwischen dem Management Server und dem Storage Node in der gleichen Weise aufgebaut wie beim Hinzufügen von Maschinen zum Server. Nachdem der Storage Node dem Management Server hinzugefügt wurde, können Sie verwaltete Depots auf dem Knoten erstellen.
Einen Storage Node vom Management Server entfernen	1. Wählen Sie den Storage Node, den Sie entfernen müssen. 2. Klicken Sie auf **Entfernen**. Nachdem der Storage Node vom Management Server entfernt wurde, verschwinden die vom Storage Node verwalteten Depots aus der Liste der Depots (S. 201) und sind danach nicht mehr für Aktionen verfügbar. Alle Pläne und Tasks, die diese Depots verwenden, werden fehlschlagen. Alle Datenbanken und Depots dieses Storage Nodes bleiben unberührt. Es ist möglich, einen bereits entfernten Storage Node dem Management Server wieder hinzuzufügen. Daraufhin werden alle vom Storage Node verwalteten Depots in der Depot-Liste angezeigt und sind wieder für alle Pläne und Tasks verfügbar, die diese Depots verwendet haben.
Ein zentrales, verwaltetes Depot auf dem ausgewählten Storage Node erstellen	1. Wählen Sie den Storage Node, der das Depot verwalten soll. 2. Klicken Sie auf **Depot erstellen**. Die Seite **Zentrales Depot erstellen** (S. 206) wird mit dem vorausgewählten Storage Node geöffnet. Führen Sie die verbleibenden Schritte zum Erstellen des Depots aus.
Details zum Storage Node anzeigen	1. Wählen Sie den Storage Node. 2. Klicken Sie auf **Details anzeigen**. Überprüfen Sie im Fenster **Storage Node-Eigenschaften** (S. 252) (dessen Inhalt auch im unteren Teil der Ansicht **Storage Nodes** und zwar im Bereich **Informationen** verfügbar ist) die Informationen zum Storage Node und den Depots, die von diesem Knoten verwaltet werden.
Verdichtung ausführen, stoppen oder neu planen	1. Wählen Sie den Storage Node. 2. Klicken Sie auf **Details anzeigen**. Klicken Sie im Fenster **Storage Node-Eigenschaften (S. 252)** auf die Links **Verdichtung starten**, **Stopp** oder **Verdichtungsplanung**.
Indizierung ausführen oder stoppen	1. Wählen Sie den Storage Node. 2. Klicken Sie auf **Details anzeigen**. Klicken Sie im Fenster **Storage Node-Eigenschaften (S. 252)** auf die Links **Indizierung starten** oder **Stopp**.

Die Liste der Storage Nodes aktualisieren	Klicken Sie auf **Aktualisieren**. Die Management Konsole aktualisiert die Liste der Storage Nodes vom Management Server mit den neuesten Informationen. Die Liste der Storage Nodes wird auf der Basis von Ereignissen automatisch aktualisiert. Möglicherweise werden die Daten dabei jedoch infolge einer gewissen Latenz nicht augenblicklich vom Management Server abgerufen. Eine manuelle Aktualisierung garantiert daher, dass auch wirklich die allerneuesten Daten angezeigt werden.

7.5.6.2 Einen Storage Node dem Management Server hinzufügen

So fügen Sie einen Storage Node hinzu

1. Geben Sie im Feld **IP/Name** den Namen oder die IP-Adresse der Maschine ein, auf der sich der Storage Node befindet – oder klicken Sie auf **Durchsuchen...**, um die Maschine aus dem Netzwerk auszuwählen.

   Benutzen Sie den vollständigen Domain-Namen (fully-qualified domain name, FQDN) des Storage Nodes, d.h., einen Domain-Namen der mit einer Top-Level Domain endet. Sie können weder „127.0.0.1 noch „localhost" als IP oder Namen des Storage Nodes verwenden. Diese Einstellungen sind auch dann nicht zu empfehlen, wenn sich Management Server und Storage Node auf der gleichen Maschine befinden, weil – nachdem der zentrale Backup-Plan unter Verwendung des Storage Nodes bereitgestellt wurde – jeder Agent versuchen wird, so auf den Storage Node zuzugreifen, als wäre dieser auf dem Host des Agenten installiert.

2. Wenn Sie ein gültiges Benutzerkonto für die Maschine angeben möchten, klicken Sie auf **Optionen>>** und geben Sie dann den folgenden Wert ein:

   - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben. Das Benutzerkonto muss Mitglied der Gruppe „Administratoren" auf der Maschine sein.
   - **Kennwort**. Das Kennwort für das Konto.

   Aktivieren Sie das Kontrollkästchen **Kennwort speichern**, um das Kennwort für das Konto zu speichern.

3. Klicken Sie auf **OK**.

Da zur Registrierung eine Beteiligung des Storage Nodes erforderlich ist, kann diese Aktion nicht ausgeführt werden, wenn die Maschine offline ist.

7.5.6.3 Eigenschaften des Storage Nodes

Im Fenster **Storage Node-Eigenschaften** werden alle Informationen zum Acronis Backup & Recovery 11.5 Storage Node in vier Registerkarten zusammengefasst. Diese Informationen sind auch im Bereich **Informationen** verfügbar.

Eigenschaften des Storage Nodes

Auf dieser Registerkarte werden die folgenden Informationen zum ausgewählten Storage Node angezeigt:

- **Name** – Der Name der Maschine, auf der der Storage Node installiert ist
- **Verfügbarkeit**:
  - **Unbekannt** – Dieser Status wird so lange angezeigt, bis nach dem Hinzufügen des Storage Nodes zum ersten Mal eine Verbindung zwischen dem Management Server und dem Storage Node hergestellt wird oder bis der Dienst des Management Servers gestartet wird.

    - **Online** – Der Storage Node ist für den Management Server verfügbar. Dies bedeutet, dass die letzte Verbindung des Management Servers mit dem Knoten erfolgreich war. Die Verbindung wird alle 2 Minuten aufgebaut.
    - **Offline** – Der Storage Node ist nicht verfügbar.
    - **Zurückgezogen** – Der Storage Node wurde auf einem anderen Management Server registriert. In diesem Fall ist es nicht möglich, den Knoten vom aktuellen Management Server aus zu steuern.
- **IP** – Die IP-Adresse der Maschine, auf der der Storage Node installiert ist.
- **Archive** – Die Gesamtzahl aller Archive, die in allen vom Storage Node verwalteten Depots gespeichert sind.
- **Backups** – Die Gesamtzahl aller Backups, die in den Archiven aller vom Storage Node verwalteten Depots gespeichert sind.
- **Indizierung** – die Indizierungsaktivität dedupliziert die Daten, die während eines Backups zu einem deduplizierenden Depot dort gespeichert werden. Die Indizierung wird immer nach Abschluss eines Backups ausgeführt. Zu weiteren Informationen über Indizierung siehe 'So funktioniert Deduplizierung (S. 260)'.
    - **Inaktiv** – es läuft gerade keine Indizierung. Sie können die Indizierung starten, indem Sie auf den Link **Indizierung starten** klicken.
    - **Läuft** – die Indizierung wird gerade ausgeführt. Sie können die Indizierung beenden, indem Sie auf den Link **Stopp** klicken. Da die Indizierung eine ressourcenverbrauchende Aktion ist, können Sie diese auf Wunsch stoppen, wenn Sie anderen, gerade wichtigeren Prozessen mehr Ressourcen zuweisen wollen. Wir empfehlen, eine Indizierung nur zu stoppen, wenn es absolut notwendig ist und sie danach so schnell wie möglich neu zu starten. Je länger Sie die Indizierung aussetzen, desto weniger Daten werden im Depot dedupliziert und desto größer ist die Speicherplatzbelegung.
- **Verdichtung** – der Verdichtungstask löscht diejenigen Blöcke aus dem Deduplizierungsdatenspeicher, auf die es keinen Bezug mehr gibt. Zu weiteren Informationen über Verdichtung siehe den Abschnitt 'So funktioniert Deduplizierung (S. 260)'.
    - **Inaktiv** – es läuft gerade keine Verdichtung. Sie können die Verdichtung starten, indem Sie auf den Link **Verdichtung starten** klicken.
    - **Läuft** – eine Verdichtung wird gerade ausgeführt. Sie können die Verdichtung beenden, indem Sie auf den Link **Stopp** klicken.
- **Verdichtungsplanung** – die Planungsparameter des Verdichtungstasks. Klicken Sie auf den Link **Verdichtungsplanung**, um den Verdichtungstask neu zu planen. Nur die Zeitereignisse (tдgliche (S. 90), wцchentliche (S. 92) und monatliche (S. 94) Planungen) können eingerichtet werden. Voreinstellung ist: Task starten jede **1 Woche** am **Sonntag** um **03:00:00 Uhr**.

Statistiken

Diese Registerlasche präsentiert Informationen über die Größe der ursprünglichen und gesicherten Daten auf allen verwalteten Depots des gewählten Storage Nodes.

Depots

Auf dieser Registerkarte wird eine Liste der Depots angezeigt, die vom gewählten Storage Node verwaltet werden. Klicken Sie auf **Aktualisieren**, damit die Liste der Depots mit den neuesten Informationen vom Management Server aktualisiert wird.

Indizierung

Diese Registerlasche ermöglicht Ihnen, den aktuellen Status der Indizierung für die deduplizierenden Depots des Storage Nodes sowie den Zeitpunkt der letzten Ausführung zu überprüfen.

7.5.6.4 Konfiguration eines Storage Nodes mit dem Acronis Administrative Template

Der nachfolgende Abschnitt erläutert die Parameter des Acronis Backup & Recovery 11.5 Storage Nodes, die unter Verwendung des Acronis Administrative Template konfiguriert werden können. Zu Informationen, wie Sie die administrative Vorlage anwenden, siehe So laden Sie das Acronis Administrative Template (S. 444).

Auf Verdichtung bezogene Parameter

Werden Backups von einem deduplizierenden Depot gelöscht, dann können in dessen Deduplizierungsdatenspeicher (S. 260) unbenutzte Datenblöcke (Elemente) verbleiben, die keinen Bezug mehr zu irgendeinem Backup haben. Der Storage Node verarbeitet den Datenspeicher, um die ungenutzten Elemente zu löschen. Diese Aktion wird 'Verdichten' bzw. 'Verdichtung' genannt. Die Durchführung einer Verdichtung erfolgt durch einen entsprechenden Verdichtungstask.

Bei jedem Start des Verdichtungstasks überprüft der Storage Node, ob eine Verdichtung durchgeführt werden muss. Der Storage Node tut dafür Folgendes:

1. Er überprüft die Größe der gesicherten Daten, die seit der letzten Verdichtung aus dem Depot gelöscht wurden.
2. Er verwendet den Parameter **Compacting Trigger Rough Estimation Threshold**, um zu bestimmen, ob diese Größe im Vergleich zur Größe der verbliebenen gesicherten Daten signifikant ist.
3. Falls das zutrifft, verwendet er den Parameter **Compacting Trigger Threshold**, um zu bestimmen, ob der Deduplizierungsdatenspeicher eine signifikante Anzahl ungenutzter Elemente enthält. Falls auch das zutrifft, führt der Storage Node die Verdichtung durch.

Die Parameter sind wie folgt.

Compacting Trigger Rough Estimation Threshold

Beschreibung: Spezifiziert die relative Größe der im Deduplizierungsdatenspeicher verbleibenden Backup-Daten, bei deren Unterschreitung eine Überprüfung auf ungenutzte Elemente erfolgt (siehe den Parameter **Compacting Trigger Threshold**).

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **100**

Standardwert: **90**

Der Parameter **Compacting Trigger Rough Estimation Threshold** ermöglicht Ihnen, die Überprüfung auf ungenutzte Elemente zu überspringen (und damit auch die Verdichtung zu überspringen), sofern sich der Inhalt des Depots nicht signifikant geändert hat.

Je größer der Wert dieses Parameters, desto häufiger wird die Überprüfung auf ungenutzte Elementen durchgeführt. Ein Wert von **100** bedeutet, dass die Überprüfung bei jedem Start des Verdichtungstasks durchgeführt wird.

Die Funktionsweise. Angenommen, der Parameterwert beträgt **90** und das Depot enthält 100 GB an Backup-Daten. Es ist nicht relevant, ob diese Daten Duplikate enthalten. Sie löschen dann einige Backups, worauf die Größe der Backup-Daten 80 GB erreicht. In diesem Fall geschieht Folgendes:

Die Größe der gelöschten Daten beträgt 20 GB, die Größe der verbliebenen Daten 80 GB. Das Verhältnis der gelöschten zu den verbliebenen Daten beträgt daher 20 GB / 80 GB = 0,25 oder 25 Prozent.

Der Storage Node kalkuliert die relative Größe der verbliebenen Daten mit der einfachen Berechnung: 100 Prozent – 25 Prozent = **75** Prozent.

Da diese relative Größe unter **90** Prozent liegt, beginnt der Storage Node mit einer Überprüfung auf ungenutzte Elemente.

Compacting Trigger Threshold

Beschreibung: Spezifiziert den Prozentsatz genutzter Elemente im Deduplizierungsdatenspeicher, unterhalb dessen die Verdichtung stattfindet.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **100**

Standardwert: **90**

Da Verdichtung eine ressourcenverbrauchende Aktion ist, sollte sie nur stattfinden, wenn die Anzahl ungenutzter Elemente signifikant ist.

Der Parameter **Compacting Trigger Threshold** ermöglicht Ihnen, eine Balance zwischen dem für die ungenutzten Elemente benötigten zusätzlichen Speicherplatz und der Verdichtungshäufigkeit einzustellen. Je größer der Wert dieses Parameters, desto weniger ungenutzte Elemente sind im Datenspeicher erlaubt – vermutlich ist jedoch eine häufigere Verdichtung notwendig.

Die Überprüfung erfolgt nur, nachdem der Prozentsatz der im Depot verbleibenden Backup-Daten ermittelt wurde (siehe **Compacting Trigger Rough Estimation Threshold**).

Andere Parameter

Log-Bereinigungsregeln

Spezifizieren Sie, wie das Log des Storage Nodes bereinigt werden soll.

Dieser Parameter hat die folgenden Einstellungen:

Maximale Größe

Beschreibung: Spezifiziert die maximale Größe des Log-Ordners für den Storage Node in Kilobyte.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **2.147.483.647**

Standardwert: **1048576** (1 GB)

Zu erhaltender Anteil

Beschreibung: Spezifiziert die maximale Log-Größe in Prozent, die bei der Bereinigung zu erhalten ist.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **100**

Standardwert: **95**

Client Connection Limit

Beschreibung: Spezifiziert die maximale Zahl gleichzeitiger Verbindungen zum Storage Node durch die Agenten, die Backup- oder Recovery-Aktionen oder Aktionen mit Archiven ausführen (etwa eine Validierung, Replikation oder Bereinigung).

*Mögliche Werte:*Jede ganze Zahl zwischen **1** und **2.147.483.647**

Standardwert: **10**

Acronis Backup & Recovery 11.5 Agenten verbinden sich mit dem Storage Node, um bei Backup- oder Recovery-Aktionen auf seine verwalteten Depots zuzugreifen oder eine Aktion mit einem Archiv durchzuführen. Der Parameter **Client Connection Limit** bestimmt die maximale Zahl solcher Verbindungen, die der Storage Node simultan handhaben kann.

Wenn diese Grenze erreicht ist, wird der Storage Node die Backup-Warteschlange (siehe Parameter) für die Agenten benutzen, die Verbindung erwarten.

Siehe auch den Parameter **Fast Operation Connection Limit**.

Backup Queue Limit

Beschreibung: Spezifiziert die maximale Zahl von Agenten in der Backup-Warteschlange des Storage Nodes.

*Mögliche Werte:*Jede ganze Zahl zwischen **1** und **2.147.483.647**

Standardwert: **50**

Die Backup-Warteschlange ist eine Liste von Agenten, die auf eine Verbindung zum Storage Node warten, um Backup- bzw. Recovery-Aktionen oder eine Aktion mit Archiven auszuführen (siehe vorherigen Parameter). Diese Liste enthält außerdem die Agenten, die aus diesen Gründen aktuell mit dem Storage Node verbunden sind.

Falls ein Agent versucht, eine solche Verbindung zu erstellen, wenn die Zahl der Agenten in der Backup-Warteschlange dem Wert von **Backup Queue Limit** entspricht, dann stellt der Storage Node diesen Agenten nicht mehr in die Warteschlange.

In diesem Fall schlägt die Verbindung des Agenten zum Storage Node fehl. Der entsprechende Task stoppt mit dem Status **Fehler**.

Siehe auch den Parameter **Fast Operation Queue Limit**.

Fast Operation Connection Limit

Beschreibung: Spezifiziert die maximale Zahl gleichzeitiger Verbindungen zum Storage Node deren Zweck andere sind als die Durchführung von Backup- bzw. Recovery-Aktionen oder andere Aktionen mit Archiven.

*Mögliche Werte:*Jede ganze Zahl zwischen **1** und **2.147.483.647**

Standardwert: **10**

Die Komponenten von Acronis Backup & Recovery 11.5 können sich mit dem Storage Node verbinden, um den Inhalt eines Depots einzusehen oder andere schnelle Aktionen auszuführen. Der Parameter **Fast Operation Connection Limit** bestimmt die maximale Zahl solcher Verbindungen, die der Storage Node gleichzeitig handhaben kann.

Wenn dieser Grenzwert erreicht wird, wird der Storage Node eine Warteschlange für schnelle Aktionen ('Fast Operations Queue' genannt, siehe nächsten Parameter) für die auf Verbindung wartenden Komponenten verwenden.

Siehe auch den Parameter **Client Connection Limit**.

Fast Operation Queue Limit

Beschreibung: Spezifiziert die maximale Zahl von Acronis Backup & Recovery 11.5-Komponenten in der Warteschlange für schnelle Aktionen (Fast Operations Queue, siehe nächsten vorherigen Parameter).

*Mögliche Werte:*Jede ganze Zahl zwischen **1** und **2.147.483.647**

Standardwert: **50**

Die Warteschlange für schnelle Aktionen ist eine Liste von Komponenten, die auf eine Verbindung zur Durchführung schneller Aktionen (etwa den Inhalt des Depots einzusehen) warten.

Sollte die Zahl der Komponenten in dieser Warteschlange dem Wert von **Fast Operation Queue Limit** entsprechen und eine weitere Komponente versuchen, eine Verbindung aufzubauen, so stellt der Storage Node diese Komponente nicht mehr in die Warteschlange. In diesem Fall schlägt die entsprechende Aktion fehl.

Siehe auch den Parameter **Backup Queue Limit**.

Vault Metadata Databases Path

Beschreibung: Spezifiziert den Pfad zu dem Ordner, wo die Depot-Datenbanken, auch Metadaten-Datenbanken genannt, gespeichert werden.

*Mögliche Werte:*Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: Leere Zeichenfolge

Eine leere Zeichenfolge entspricht dem Ordner '%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\ASN\VaultMetadataDatabases' (in Windows XP und Server 2003) oder '%PROGRAMDATA%\Acronis\BackupAndRecovery\ASN\VaultMetadataDatabases' (in Windows Vista und späteren Versionen von Windows).

Eine Depot-Datenbank enthält Informationen über alle im Depot gespeicherte Archive und Backups. Wenn Sie ein Depot erstellen oder anschließen, platziert der Storage Node die Datenbank für dieses Depot in dem Ordner, der durch diesen Parameter bestimmt wird.

Eine Änderung dieses Parameters hat keinen Einfluss auf aktuell existierende Depot-Datenbanken. Falls Sie wollen, dass diese Datenbanken zu dem neuen Ordner verschoben werden, dann trennen (S. 204) Sie die entsprechenden Depots und schließen (S. 211) Sie diese dann an denselben Storage Node an.

Pfad zur Deduplizierungsdatenbank

Beschreibung: Spezifiziert den Pfad, wo die jeweilige Deduplizierungsdatenbank gespeichert ist.

*Mögliche Werte:*Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: Leere Zeichenfolge

Eine leere Zeichenkette bedeutet, dass der Pfad manuell eingegeben werden muss.

Eine Deduplizierungsdatenbank enthält die Hash-Werte aller in einem Depot vorliegenden Datenelemente – mit Ausnahme von nicht deduplizierbaren Daten. Wenn Sie ein deduplizierendes Depot erstellen, platziert der Storage Node die Deduplizierungsdatenbank für dieses Depot in dem Ordner, der durch diesen Parameter bestimmt wird. Platzieren Sie die Datenbank zur Performance-Optimierung auf einem anderen Laufwerk als dem, welches zur Backup-Speicherung verwendet wird.

Eine Änderung dieses Parameters hat keinen Einfluss auf aktuell existierende Deduplizierungsdatenbanken.

Check Hash Value On Server Side

Beschreibung: Spezifiziert, ob die Hash-Werte der Datenblöcke überprüft werden sollen, die an ein deduplizierendes Depot übertragen werden.

Mögliche Werte: **Aktiviert** oder **Deaktiviert**

Standardwert: **Deaktiviert**

Wenn Sie einen Datenblock an ein deduplizierendes Depot senden, sendet der Agent außerdem den 'Fingerabdruck' (Hash-Wert) dieses Blocks mit.

Der Parameter **Check Hash Value On Server Side** bestimmt, ob der Storage Node sicherstellen soll, dass der Hash-Wert zu dem Datenblock passt. Eine solche Überprüfung verursacht eine zusätzliche Last auf dem Storage Node.

Normalerweise ist eine solche Überprüfung nicht notwendig. Sie können diesen Parameter aber auf **Aktiviert** einstellen, um den Deduplizierungsprozess sicherer zu machen.

Falls die Überprüfung eine Nichtübereinstimmung zwischen einem Datenblock und seinem Hash-Wert aufdeckt, schlägt die Backup-Aktion fehl.

Depot-Warnungen und -Beschränkungen

Spezifiziert die Menge freien Speicherplatzes in einem Depot (als absoluten Wert und prozentual) bei deren Unterschreitung ein Fehler im Log aufgezeichnet wird.

Dieser Parameter enthält folgende Einstellungen:

Vault Free Space Warning Limit

Beschreibung: Spezifiziert die Menge freien Speicherplatzes in einem verwalteten Depot (in Megabyte) bei deren Unterschreiten eine Warnmeldung in die Ereignisanzeige des Storage Nodes aufgenommen wird.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **2.147.483.647**

Standardwert: **200**

Der freie Speicherplatz eines Depots ist die Menge freien Speicherplatzes eines Mediums, etwa ein Laufwerk-Volume, welches das Depot enthält.

Falls die Menge freien Speicherplatzes in einem Depot einen Wert erreicht, der gleich oder geringer ist als unter **Vault Free Space Warning Limit** angegeben, wird eine Warnmeldung in die Ereignisanzeige des Depots aufgenommen und so auf das betreffende Depot hingewiesen. Sie können die Warnmeldungen des Storage Nodes im Dashboard einsehen.

Vault Free Space Warning Percentage

Beschreibung: Spezifiziert die Menge freien Speicherplatzes in einem verwalteten Depot (in Prozent seiner Gesamtgröße) bei deren Unterschreitung eine Warnmeldung in die Ereignisanzeige des Storage Nodes aufgenommen wird.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **100**

Standardwert: **10**

Die Gesamtgröße eines Depots entspricht seinem freien Speicherplatz plus der Größe aller in diesem Depot enthaltenen Archive.

Ein Beispiel: Angenommen, zwei Depots, Depot A und Depot B, sind beide auf einem Laufwerk gespeichert. Nehmen Sie weiter an, die Größe der Archive im Depot A ist 20 GB ist und die Größe der Archive im Depot B beträgt 45 GB.

Sollte das Laufwerk 5 GB freien Speicherplatz haben, so beträgt die Gesamtgröße des Depots A 20 GB + 5 GB = 25 GB und die des Depots B 45 GB + 5 GB = 50 GB – unabhängig von der Größe des Laufwerkes.

Der Prozentsatz an freiem Speicherplatz eines Depots entspricht seinem freien Platz geteilt durch seine Gesamtgröße. In Bezug auf das vorherige Beispiel entspricht das beim Depot A 5 GB / 25 GB = 20% an freien Speicherplatz – während Depot B 5 GB / 50 GB = 10% an freiem Speicherplatz hat.

Falls der Prozentsatz an freiem Platz in einem Depot einen Wert erreicht, der gleich oder geringer ist als unter **Vault Free Space Warning Percentage** angegeben, wird eine Warnmeldung in die Ereignisanzeige des Depots aufgenommen und so auf das betreffende Depot hingewiesen. Sie können die Warnmeldungen des Storage Nodes im Dashboard einsehen.

Hinweis: *Die Parameter* ***Vault Free Space Warning Limit*** *und* ***Vault Free Space Warning Percentage*** *sind unabhängig voneinander. Jedes Mal, wenn einer der beiden Schwellenwerte erreicht wird, wird eine Warnmeldung aufgenommen.*

Vault Free Space Error Limit

Beschreibung: Spezifiziert die Menge freien Speicherplatzes in einem verwalteten Depot (in Megabyte) bei deren Unterschreitung eine Fehlermeldung in die Ereignisanzeige des Storage Nodes aufgenommen wird und jedes Backup zum Depot unterbunden wird.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **2.147.483.647**

Standardwert: **50**

Falls die Menge freien Platzes in einem Depot einen Wert erreicht, der gleich oder geringer ist als unter **Vault Free Space Error Limit** angegeben, wird eine Fehlermeldung in die Ereignisanzeige des Depots aufgenommen. Backups, die in das Depot ausgeführt werden, werden solange scheitern, bis der freie Platz des Depots wieder über dem Limit liegt.

Vault Database Free Space Warning Limit

Beschreibung: Spezifiziert die Menge freien Speicherplatzes (in Megabyte) eines Laufwerks, welches die Datenbank eines verwalteten Depots enthält, bei deren Unterschreitung eine Warnmeldung in die Ereignisanzeige des Storage Nodes aufgenommen wird.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **2.147.483.647**

Standardwert: **20**

Falls die Menge freien Speicherplatzes auf dem Volume, welches die Datenbank eines verwalteten Depots enthält, einen Wert erreicht, der gleich oder geringer ist als unter **Vault Database Free Space Warning Limit** angegeben, wird eine Warnmeldung in die Ereignisanzeige des Storage Nodes aufgenommen und so auf das betreffende Depot hingewiesen. Sie können die Warnmeldungen des Storage Nodes im Dashboard einsehen.

Die Datenbank wird auf dem Storage Node in einem lokalen Ordner gespeichert, dessen Name durch den Parameter **Vault Metadata Database Path** spezifiziert wird.

Vault Database Free Space Error Limit

Beschreibung: Spezifiziert die Menge freien Speicherplatzes (in Megabyte) eines Laufwerks, welches die Datenbank eines verwalteten Depots enthält, bei deren Unterschreitung eine Warnmeldung in die Ereignisanzeige des Storage Nodes aufgenommen wird und jedes weitere Backup zum Depot unterbunden wird.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **2.147.483.647**

Standardwert: **10**

Falls die Menge freien Platzes auf dem Laufwerk, das die Datenbank eines verwalteten Depots enthält, einen Wert erreicht, der gleich oder geringer ist als unter **Vault Database Free Space Error Limit** angegeben, wird eine Fehlermeldung in die Ereignisanzeige des Storage Nodes aufgenommen. Backups, die in das Depot ausgeführt werden, werden solange scheitern, bis der freie Platz wieder über dem Limit liegt.

Sie können die Fehlermeldungen des Storage Nodes im Dashboard einsehen.

Die Datenbank wird auf dem Storage Node in einem lokalen Ordner gespeichert, dessen Name durch den Parameter **Vault Metadata Database Path** spezifiziert wird.

7.5.7 Deduplizierung

Dieser Abschnitt beschreibt den Deduplizierungsmechanismus, der entwickelt wurde, um Datenwiederholungen dadurch zu eliminieren, dass identische Daten in Archiven nur noch einmal gespeichert werden.

7.5.7.1 Überblick

Deduplizierung ist ein Prozess zur Minimierung von durch Daten belegten Speicherplatz, indem Daten-Wiederholungen erkannt werden und identische Daten nur noch einmal gespeichert werden.

Deduplizierung kann außerdem die Netzwerklast reduzieren: Sollte während eines Backups Daten gefunden werden, die Duplikate von bereits gespeicherten Daten sind, so wird ihr Inhalt nicht noch einmal über das Netzwerk übertragen.

Acronis Backup & Recovery 11.5 wird zu einem verwalteten Depot gespeicherte Backups nur dann deduplizieren, falls Sie während der Depot-Erstellung die Deduplizierungsfunktion aktiviert haben. Ein Depot mit aktivierter Deduplizierung wird **deduplizierendes Depot** genannt. Das Deduplizierungs-Add-on für den Agenten muss auf jeder Maschine installiert werden, die Backups zu einem solchen Depot erstellt. Ohne dieses Add-on sind keine Backups zu dem Depot möglich.

Das Objekt der Deduplizierung sind Datenblöcke. Die Größe dieser Blöcke beträgt **4 KB für Laufwerk-Backups** und **1 B bis 256 KB für Datei-Backups**. Jede Datei, die kleiner ist als 256 KB wird als ein Datenblock betrachtet. Dateien, die größer sind als 256 KB, werden in 256-KB-Blöcke aufgeteilt.

Eine Deduplizierung wird von Acronis Backup & Recovery 11.5 in zwei Schritten durchgeführt:

Deduplizierung an der Quelle

Die Durchführung erfolgt während eines Backups auf einer verwalteten Maschine. Der Agent verwendet den Storage Node, um zu bestimmen, welche Daten dedupliziert werden können und überträgt dann keine Datenblöcke mehr, deren Duplikate bereits im Depot vorliegen.

Deduplizierung am Ziel

Durchführung im Depot nach Fertigstellung eines Backups. Der Storage Node analysiert den Inhalt des Depots und dedupliziert dann die dort befindlichen Daten.

Sie erhalten beim Erstellen eines Backup-Plans die Option, die Deduplizierung an der Quelle auszuschalten. Das kann zu schnelleren Backups führen, aber auch zu größerer Last für das Netzwerk und den Storage Node.

Deduplizierungsdatenbank

Ein Acronis Backup & Recovery 11.5 Storage Node, der ein deduplizierendes Depot verwaltet, hält eine Deduplizierungsdatenbank aufrecht, die die Hash-Werte aller im Depot vorliegenden Datenblöcke enthält (mit Ausnahme solcher, die nicht deduplizierbar sind, etwa verschlüsselte Dateien).

Die Deduplizierungsdatenbank wird in einem lokalen Ordner des Storage Nodes gespeichert. Sie können den Pfad zur Datenbank bei Erstellung des Depots spezifizieren.

Die Größe einer Deduplizierungsdatenbank beträgt ungefähr 1,5 Prozent der Gesamtgröße aller im Depot gespeicherten 'einmaligen Daten'. Mit anderen Worten, jedes Terabyte an neuen (nicht doppelten) Daten fügt der Datenbank ca. 15 GB hinzu.

Sollte eine Datenbank beschädigt sein oder der Storage Node verloren gehen, während der Inhalt des Depots bestehen bleibt, so scannt der neue Storage Node das Depot und erstellt die Datenbank wieder neu.

7.5.7.2 So funktioniert Deduplizierung

Deduplizierung an der Quelle

Während der Backup-Erstellung zu einem deduplizierenden Depot berechnet der Acronis Backup & Recovery 11.5 Agent für jeden Datenblock einen so genannten Fingerabdruck. Ein solcher Fingerabdruck wird auch als *Hash-Wert* bezeichnet.

Bevor ein Datenblock zum Depot übertragen wird, fragt der Agent die Deduplizierungsdatenbank ab, um zu bestimmen, ob der Hash-Wert dieses Blocks dem eines bereits gespeicherten Blocks entspricht. Trifft dies zu, dann überträgt der Agent nur den Hash-Wert, wenn nicht, dann wird der

Block selbst übertragen. Der Storage Node speichert die empfangenen Datenblöcke in einer temporären Datei.

Einige Daten, etwa verschlüsselte Dateien oder Laufwerksdatenblöcke mit nicht standardkonformer Größe, können nicht dedupliziert werden. Solche Daten werden vom Agenten immer ohne Berechnung ihrer Hash-Werte zum Depot übertragen. Mehr Informationen über Beschränkungen bei der Deduplizierung finden Sie unter Deduplizierungsbeschrдnkungen (S. 265).

Sobald der Backup-Prozess abgeschlossen wurde, sind im Depot das resultierende Backup sowie die temporäre Datei mit den einmaligen Datenblöcken enthalten. Die temporäre Datei wird dann in der nächsten Phase verarbeitet. Das Backup (eine tib-Datei) enthält Hash-Werte zusammen mit Daten, die nicht dedupliziert werden können. Eine weitere Verarbeitung dieses Backups ist nicht notwendig. Sie können ohne Weiteres Daten aus diesem wiederherstellen.

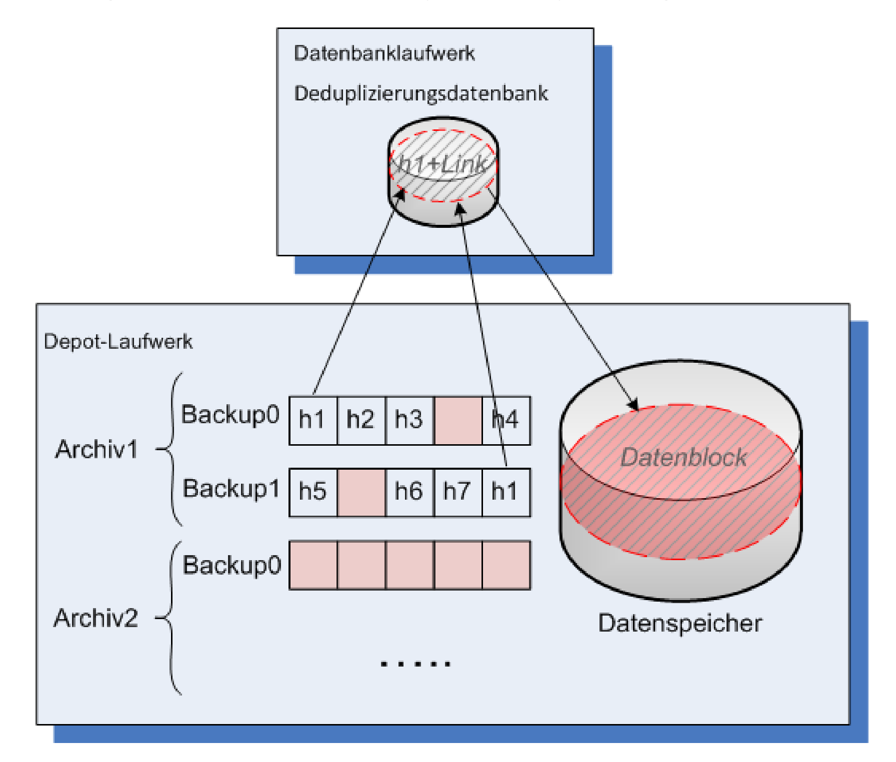
Deduplizierung am Ziel

Nachdem ein Backup zu einem deduplizierenden Depot abgeschlossen wurde, führt der Storage Node eine **Indizierungsaktivität** aus. Durch diese Aktivität werden die Daten in dem Depot folgendermaßen dedupliziert:

1. Die Datenblöcke werden aus der temporären Datei in eine spezielle Datei innerhalb des Depots verschoben, in der doppelt vorhandene Elemente dann nur noch einmal gespeichert werden. Diese Datei wird **Deduplizierungsdatenspeicher** genannt.
2. Sie speichert die Hash-Werte und Links, die zum Zusammensetzen der deduplizierten Daten für die Deduplizierungsdatenbank notwendig sind.
3. Nachdem alle Datenblöcke verschoben wurden, wird die temporäre Datei gelöscht.

Als Ergebnis enthält der Datenspeicher eine bestimmte Anzahl an einmaligen Datenblöcken. Von den Backups gibt es einen oder mehrere Verweise auf jeden Block. Die Verweise sind in der Deduplizierungsdatenbank enthalten. Die Backups selbst verbleiben unberührt. Sie enthalten Hash-Werte sowie Daten, die nicht dedupliziert werden können.

Das nachfolgende Diagramm illustriert das Prinzip der Deduplizierung am Ziel.



Eine Indizierungsaktivität kann eine beträchtliche Zeit zur Fertigstellung benötigen. Sie können das Stadium dieser Aktivität auf dem Management Server einsehen, wenn Sie den entsprechenden Storage Node auswählen und auf **Details anzeigen** (S. 252) klicken. Sie können diese Aktivität in dem Fenster auch manuell starten oder stoppen.

Verdichten

Wurden ein oder mehrere Backups bzw. Archive vom Depot gelöscht (entweder manuell oder durch Bereinigung), so kann der Datenspeicher Datenblöcke enthalten, auf die sich keine Archive mehr beziehen. Solche Blöcke werden dann durch einen **Verdichtungstask** gelöscht, bei dem es sich um einen geplanten, vom Storage Node ausgeführten Task handelt.

Als Standardvorgabe läuft der Verdichtungstask jeweils sonntags in der Nacht um 03:00 Uhr. Sie können den Task neu planen, indem Sie den entsprechenden Storage Node wählen, zuerst auf **Details anzeigen** (S. 252) klicken und dann auf **Verdichtungsplanung**. Sie können den Task in dieser Registerlasche auch manuell starten oder stoppen.

Da das Löschen unbenutzter Datenblöcke ein ressourcenverbrauchender Prozess ist, wird der Verdichtungstask nur ausgeführt, wenn sich eine ausreichende Datenmenge angesammelt hat. Der Grenzwert wird über den Konfigurationsparameter **Compacting Trigger Threshold** (S. 254) bestimmt.

7.5.7.3 Wann Deduplizierung am effektivsten ist

Nachfolgend einige Beispiele, wann Deduplizierung die besten Ergebnisse erzielt:

- Beim Sichern ähnlicher Daten aus verschiedenen Quellen im **Voll-Backup-Modus**. Das ist z.B. beim Backup von Betriebssystem und Anwendungen der Fall, wenn diese von einer Quelle aus per Netzwerk verteilt wurden.
- Bei Durchführung **inkrementeller Backups** von ähnlichen Daten aus verschiedenen Quellen unter der Annahme, dass **die Daten-Veränderungen ebenfalls ähnlich sind**. Das ist z.B. der Fall, wenn Sie Updates zu diesen Systemen verteilen und auf diese dann das inkrementelle Backup anwenden.
- Bei Durchführung von **inkrementellen Backups** von Daten, die sich nicht selbst, aber **ihren Speicherplatz geändert** haben. Das ist z.B. der Fall, wenn multiple Teile von Daten durch das Netzwerk oder innerhalb eines Systems zirkulieren. Jedes Mal, wenn ein Teil dieser Daten verschoben wird, wird dieser in das inkrementelle Backup aufgenommen, welches an Größe zunimmt, während es aber keine neuen Daten enthält. Deduplizierung hilft, dieses Problem zu lösen: Jedes Mal, wenn ein Element an einem neuen Ort erscheint, wird statt des Elements selbst eine Referenz auf dieses gespeichert.

Deduplizierung und inkrementelle Backups

Bei zufälliger Veränderung von Daten führt die Deduplizierung daraus resultierender inkrementeller Backups zu keinem großen Effekt, denn:

- Die deduplizierten Elemente, die sich nicht verändert haben, sind in den inkrementellen Backups nicht enthalten.
- Die deduplizierten Elemente, die sich nicht verändert haben, sind nicht mehr identisch und werden daher auch nicht dedupliziert.

Deduplizierung und Datenbank-Backups

Deduplizierung ist zum regelmäßigen Backup einer Datenbank nicht besonders effektiv. Hintergrund ist, dass Änderungen an einer Datenbank meistens einzigartig sind und daher nicht dedupliziert

werden können. Wir empfehlen daher, Datenbanken zu einem nicht-deduplizierenden Depot zu sichern.

7.5.7.4 Optimale Vorgehensweisen bei der Deduplizierung

Deduplizierung ist ein komplexer Prozess, der von vielen Faktoren abhängt.

Die wichtigsten Faktoren, die die Deduplizierungsgeschwindigkeit beeinflussen, sind:

- Die Zugriffsgeschwindigkeit auf die Deduplizierungsdatenbank
- Die RAM-Kapazität des Storage Nodes
- Die Anzahl der deduplizierenden Depots, die auf dem Storage Node erstellt wurden.

Folgen Sie den unteren Empfehlungen, um die Deduplizierungsperformance zu verbessern.

Legen Sie die Deduplizierungsdatenbank und das deduplizierende Depot auf separate physikalische Geräte

Um die Zugriffsgeschwindigkeit auf eine Deduplizierungsdatenbank verbessern zu können, müssen die Datenbank und das Depot auf separaten physikalischen Geräten liegen.

Es ist am besten, dem Depot und der Datenbank je eigene, nur dafür dedizierte Geräte zuzuweisen. Falls das nicht möglich ist, sollten Sie zumindest weder das Depot noch die Datenbank auf ein gemeinsames Laufwerk mit dem Betriebssystem legen. Der Grund ist, dass das Betriebssystem häufige Lese-/Schreib-Aktionen auf dem Laufwerk durchführt, was die Deduplizierung deutlich verlangsamen kann.

Ein Laufwerk für eine Deduplizierungsdatenbank auswählen

- Die Datenbank muss auf einem fest eingebauten Laufwerk liegen. Versuchen Sie nicht, die Deduplizierungsdatenbank auf ein externes, entfernbares Laufwerk zu legen.
- Eine möglichst schnelle Zugriffszeit ist wichtig. Es wird empfohlen, eine schnelle IDE-Festplatte (7200 Upm oder schneller), ein SCSI-Laufwerk oder eine für den Unternehmenseinsatz ausgelegte SSD (Solid State Drive) zu verwenden.
- Das zur Speicherung der Deduplizierungsdatenbank verwendete Volume sollte mindestens 10 GB an freien Speicherplatz haben. Wenn Sie eine große Anzahl von Maschinen sichern, dürfte der benötigte freie Speicherplatz die 10 GB überschreiten.
- Der für eine Deduplizierungsdatenbank erforderliche Speicherplatz kann mit folgender Formel abgeschätzt werden:

  $$G = E / 32 + 10$$

  wobei gilt:

  G – die Laufwerksgröße in GB ist,

  E – die geplante Menge an 'einmaligen' (nur einmal vorkommenden) Daten im Deduplizierungsdatenspeicher in GB ist.

  Falls beispielsweise für die geplante Menge der einmaligen Daten im Deduplizierungsdatenspeicher 'E=5 TB' gilt, dann erfordert die Deduplizierungsdatenbank einen freien Speicherplatz, der nicht kleiner ist als

  $$G = 5*1024 / 32 + 10 = 170 \text{ GB}$$

Ein Laufwerk für ein deduplizierendes Depot wählen

Zum Schutz gegen Datenverlust empfehlen wir die Verwendung von RAID 10, 5 oder 6. RAID 0 wird nicht empfohlen, da es nicht fehlertolerant ist. RAID 1 ist aufgrund seiner geringen Geschwindigkeit nicht empfehlenswert. Es gibt keine Bevorzugung von lokalen Laufwerken gegenüber SAN, beide sind gut.

8 GB an RAM pro 1 TB an einmaligen Daten.

Das ist eine Empfehlung für ein 'Worst Case'-Szenario. Sie müssen dem nicht unbedingt folgen, solange Sie keine Performance-Probleme bei der Deduplizierung feststellen. Sollte die Deduplizierung jedoch zu langsam ablaufen, dann überprüfen Sie den Parameter **Belegter Speicherplatz** des deduplizierenden Depots. Sie können die Deduplizierungsgeschwindigkeit signifikant anheben, indem Sie den Arbeitsspeicher (RAM) des Storage Nodes vergrößern.

Im Allgemeinen gilt, dass bei gleicher Deduplizierungsgeschwindigkeit die Größe der Deduplizierungsdatenbank umso größer sein kann, je mehr RAM Sie haben.

Nur ein deduplizierendes Depot auf jedem Storage Node

Es wird dringend empfohlen, nur ein deduplizierendes Depot auf einem Storage Node zu erstellen. Anderenfalls wird die gesamte Menge des RAMs proportional zur Anzahl der Depots unter diesen aufgeteilt.

64-Bit-Betriebssystem

Der Storage Node muss unter einem 64-Bit-Betriebssystem installiert werden. Auf der Maschine mit dem Storage Node sollten keine weiteren Anwendungen ausgeführt werden, die viele Systemressourcen erfordern, wie beispielsweise Datenbankverwaltungssysteme (DBMS) oder Enterprise Resource Planning-Systeme (ERP).

Mehrkern-Prozessor mit einer Taktrate von mindestens 2,5 GHz

Wir empfehlen die Verwendung eines Prozessors mit wenigstens 4 Kernen und einer Taktfrequenz nicht unter 2,5 GHz.

Ausreichend freier Speicherplatz im Depot

Die Indizierung eines Backups erfordert genauso viel freien Speicherplatz, wie die Daten des Backups unmittelbar nach ihrer Sicherung zum Depot belegt haben. Ohne Komprimierung oder Deduplizierung an der Quelle entspricht dieser Wert der Größe der ursprünglich gesicherten Daten während einer gegebenen Backup-Aktion.

High-Speed LAN

1-Gbit-LAN wird empfohlen. Dadurch kann die Software 5-6 Backups mit Deduplizierung parallel durchführen, ohne dass die Geschwindigkeit deutlich heruntergeht.

Backup einer typischen Maschine, bevor Sie mehrere Maschinen mit ähnlichem Inhalt sichern

Wenn Sie mehrere Maschinen mit ähnlichem Inhalt sichern wollen, empfiehlt es sich, zuerst nur das Backup einer Maschine zu erstellen und dann zu warten, bis die Indizierung der gesicherten Daten abgeschlossen ist. Danach werden die Backups der anderen Maschinen schneller verlaufen, was der effizienten Deduplizierung zu verdanken ist. Da das Backup der ersten Maschine bereits indiziert wurde, befinden sich die meisten Daten bereits im Deduplizierungsdatenspeicher.

Backups von verschiedenen Maschinen zu unterschiedlichen Zeiten

Falls Sie eine größere Anzahl an Maschinen sichern wollen, sollten Sie die Backup-Aktionen zeitlich verteilen. Erstellen Sie dazu mehrere Backup-Pläne mit unterschiedlichen Planungen.

Schnelle Katalogisierung verwenden

Die Indizierung eines Backups startet, nachdem seine Katalogisierung abgeschlossen wurde. Um die zur Backup-Verarbeitung benötigte Gesamtzeit zu reduzieren, können Sie die automatische Katalogisierung (S. 119) in den schnellen Modus umschalten. Sie können die vollständige Katalogisierung auch manuell außerhalb des Backup-Fensters starten.

Alarmbenachrichtigungen konfigurieren

Es wird empfohlen, dass Sie in den Management Server-Optionen Alarmbenachrichtigungen (S. 441) für die Depots konfigurieren. Dadurch können Sie schneller bei Störungen oder Ausfällen reagieren. Eine rechtzeitige Reaktion auf eine Alarmmeldung vom Typ „Es gibt ein Depot mit wenig freiem Speicherplatz“ kann vor einem Fehler beim nächsten Backup zum Depot schützen.

7.5.7.5 Deduplizierungsbeschränkungen

Allgemeine Einschränkungen

Eine Deduplizierung kann nicht durchgeführt werden, falls Sie das Archiv mit einem Kennwort geschützt haben. Die Datenblöcke kennwortgeschützter Archive werden in den Backups so gespeichert, als wären sie in einem nicht-deduplizierenden Depot.

Falls Sie Archive unter Beibehaltung der Möglichkeit zur Deduplizierung schützen wollen, dann belassen Sie die Archive ohne Kennwortschutz und verschlüsseln Sie stattdessen das deduplizierende Depot mit einem Kennwort. Sie können dies bei Erstellung des Depots durchführen.

Backup auf Laufwerkebene

Eine Deduplizierung von Laufwerksdatenblöcken erfolgt nicht, falls die Größe der Zuordnungseinheit des Volumes – auch als Cluster-Größe oder Block-Größe bekannt – nicht durch 4 KB teilbar ist.

***Tipp:** Die Größe der Zuordnungseinheit der meisten NTFS- und ext3-Volumes beträgt 4 KB. Dies erlaubt also eine Deduplizierung auf Block-Ebene. Andere Größen von Zuordnungseinheiten, die eine Deduplizierung auf Block-Ebene ermöglichen, sind z.B. 8 KB, 16 KB und 64 KB.*

Backup auf Dateiebene

Die Deduplizierung einer Datei erfolgt nicht, falls die Datei verschlüsselt ist und das Kontrollkästchen **Verschlüsselte Dateien in Archiven unverschlüsselt speichern** deaktiviert ist (Standardeinstellung).

Deduplizierung und NTFS-Datenströme

Im NTFS-Dateisystem kann eine Datei mit einem oder mehreren zusätzlichen Datensätzen assoziiert sein – meist (englisch) *Alternate Data Streams* genannt.

Beim Backup einer solchen Datei werden auch all ihre 'Alternate Data Streams' mit gesichert. Diese Streams werden jedoch auch dann nie dedupliziert, wenn die Datei selbst es wird.

8 Aktionen mit Archiven und Backups

8.1 Archive und Backups validieren

Validierung ist eine Aktion, mit der die Möglichkeit der Datenwiederherstellung aus einem Backup geprüft wird.

Die Validierung eines Datei-Backups imitiert die Wiederherstellung aller Dateien aus einem Backup an einen imitierten Zielort. Die Validierung eines Festplatten- oder Partitions-Backups berechnet eine Prüfsumme für jeden Datenblock, der im Backup gespeichert ist. Beide Prozeduren sind ressourcenintensiv.

Die Validierung eines Archivs bestätigt die Gültigkeit aller Backups im Archiv. Die Validierung eines Depots (bzw. Speicherorts) bewirkt eine Überprüfung aller in diesem Depot (Speicherort) hinterlegten Archive.

Obwohl eine erfolgreiche Validierung eine hohe Wahrscheinlichkeit für eine erfolgreiche Wiederherstellung bedeutet, werden nicht alle Faktoren geprüft, die eine Wiederherstellung beeinflussen. Wenn Sie ein Betriebssystem gesichert haben und Sie sichergehen wollen, dass spätere Recovery-Aktionen des Backups erfolgreich sind, dann lässt sich das nur garantieren, wenn Sie eine testweise Wiederherstellung unter Verwendung einer bootfähigen Umgebung auf ein freies, ungenutztes Laufwerk durchführen. Sie sollten zumindest sicherstellen, dass das Backup unter Verwendung eines bootfähigen Mediums erfolgreich validiert werden kann.

Beschränkung
Archive und Backups im Acronis Online Backup Storage (S. 460) können nicht validiert werden. Ein 'Initial Seeding'-Backup (S. 465) wird jedoch direkt nach seiner Erstellung automatisch validiert.

Verschiedene Varianten, einen Validierungstask zu erstellen

Die Verwendung der Seite **Validation** ist der übliche Weg, um einen Validierungstask zu erstellen. Sie können hier Validierungen sofort ausführen oder eine Validierungsplanung für jedes Backup, Archiv oder Depot erstellen, auf das Sie Zugriff haben.

Die Validierung eines Archivs oder des letzten Backups in dem Archiv kann auch als Teil eines Backup-Plans durchgeführt werden. Weitere Informationen finden Sie im Abschnitt 'Einen Backup-Plan erstellen (S. 58)'.

Wählen Sie zuerst ein Objekt zur Validierung aus, um Zugriff auf die Seite **Validierung** zu erhalten: ein Depot, ein Archiv oder ein Backup.

- Klicken Sie zur Wahl eines Depots im Fensterbereich **Navigation** auf das Symbol **Depots** – und wählen Sie dann das Depot, indem Sie den Depot-Verzeichnisbaum in der Ansicht **Depots** erweitern oder es direkt im Fensterbereich **Navigation** auswählen.
- Wählen Sie zur Auswahl eines Archivs zuerst ein Depot an und dann in der Ansicht **Depot** die Registerlasche **Archiv-Anzeige** – anschließend klicken Sie auf den Namen des entsprechenden Archivs.
- Wählen Sie zur Wahl eines Backups zuerst ein Archiv aus der **Archiv-Anzeige**, erweitern Sie dann das Archiv über die entsprechende Schaltfläche links neben dem Archivnamen und klicken Sie abschließend auf das gewünschte Backup.

Klicken Sie nach Wahl des Validierungsobjektes im Kontextmenü auf den Befehl **Validieren**. Darauf öffnet sich die Seite **Validierung** mit dem vorausgewählten Objekt als Quelle. Sie müssen dann nur noch wählen, wann validiert werden soll, und (optional) einen Namen für den Tasks angeben.

Zur Erstellung eines Validierungstasks führen Sie die folgenden Schritte aus.

Validierungsquelle

Validieren

Wählen Sie ein zu validierendes Objekt:

Archiv (S. 273) – Sie müssen in diesem Fall das Archiv spezifizieren.

Backup (S. 268) - spezifizieren Sie zuerst das Archiv. Wählen Sie dann das gewünschte Backup aus dem Archiv.

Depot (S. 268) – wählen Sie ein Depot (oder einen anderen Speicherort), dessen Archive validiert werden sollen.

Anmeldedaten (S. 268)

[Optional] Stellen Sie Anmeldedaten für die Quelle zur Verfügung, falls das Benutzerkonto des Tasks dafür nicht genügend Zugriffsrechte hat.

Validierungszeitpunkt

Validierung starten (S. 269)

Geben Sie an, wann und wie oft die Validierung durchgeführt werden soll.

Task-Parameter

Task-Name

[Optional] Geben Sie einen eindeutigen Namen für den Validierungstask ein. Ein bewusst gewählter Name macht es leichter, diesen Task zu identifizieren.

Anmeldedaten des Plans: (S. 269)

[Optional] Der Validierungstask wird im Namen des Benutzers laufen, der den Task erstellt. Sie können, sofern notwendig, die Anmeldedaten für den Task ändern.

Kommentare

[Optional] Geben Sie Kommentare für den Task ein.

Nachdem Sie alle notwendigen Einstellungen konfiguriert haben, klicken Sie auf **OK**, um den Validierungstask zu erstellen.

8.1.1 Auswahl des Archivs

So spezifizieren Sie ein zu validierendes Archiv

1. Tragen Sie den vollständigen Pfad zum Archiv-Speicherort in das Feld **Pfad** ein – oder wählen Sie den gewünschten Speicherort aus dem Verzeichnisbaum (S. 149).

   Bei Ausführung auf einer Maschine, die mit einem bootfähigen Medium gestartet wurde:

   - Um auf ein verwaltetes Depot zuzugreifen, geben Sie im Feld **Pfad** ein:

     bsp://knoten_adresse/depot_name/

   - Um auf ein zentrales, nicht verwaltetes Depot zuzugreifen, tragen Sie den vollen Pfad zum Ordner des Depots ein.

2. Wählen Sie das Archiv in der Tabelle rechts vom Verzeichnisbaum. Die Tabelle zeigt die Namen der Archive, die sich in jedem von Ihnen gewählten Speicherort befinden.

   Während Sie den Inhalt eines Speicherorts untersuchen, können Archive durch einen anderen Benutzer oder das Programm (auf Basis geplanter Aktionen) hinzugefügt, gelöscht oder

modifiziert werden. Verwenden Sie die Schaltfläche **Aktualisieren**, um die Liste der Archive neu aufzubauen.

3. Klicken Sie auf **OK**.

8.1.2 Auswahl der Backups

So spezifizieren Sie ein zu validierendes Backup.

1. Wählen Sie im oberen Fensterbereich ein Backup anhand des Zeitstempels.

   Der untere Teil des Fensters zeigt den Inhalt des gewählten Backups, um Sie darin zu unterstützen, das richtige Backup herauszufinden.

2. Klicken Sie auf **OK**.

8.1.3 Depot wählen

So wählen Sie ein Depot oder einen Speicherort

1. Tragen Sie den vollständigen Pfad zum Depot (Speicherort) in das Feld **Pfad** ein – oder wählen Sie den gewünschten Speicherort aus dem Verzeichnisbaum.

- Um ein zentrales Depot auszuwählen, erweitern Sie die Gruppe **Zentral** und wählen dort dieses Depot.
- Um ein persönliches Depot auszuwählen, erweitern Sie die Gruppe **Persönlich** und klicken dann auf das entsprechende Depot.
- Um einen lokalen Ordner auszuwählen (CD-/DVD-Laufwerk oder ein lokal angeschlossenes Bandgerät), erweitern Sie die Gruppe **Lokale Ordner** und klicken auf den gewünschten Ordner.
- Um eine Netzwerkfreigabe zu wählen, erweitern Sie die Gruppe **Netzwerkordner**, wählen die benötigte Netzwerk-Maschine und klicken dann auf den freigegebenen Ordner. Werden Anmeldedaten zum Zugriff auf die Netzwerkfreigabe benötigt, so wird das Programm diese erfragen.
- Um einen Ordner auszuwählen, der auf einer NFS-Freigabe gespeichert ist, erweitern Sie die Gruppe **NFS-Laufwerke** und klicken Sie auf den entsprechenden Ordner.
- Um einen **FTP-** oder **SFTP-**Server zu wählen, erweitern Sie die korrespondierende Gruppe und wählen die entsprechenden Ordner auf dem Server.

  Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

  Die Tabelle zeigt für jedes von Ihnen gewählte Depot die Namen dort enthaltener Archive an, um Ihnen die Wahl des richtigen Depots zu erleichtern. Während Sie den Inhalt eines Speicherorts untersuchen, können Archive durch einen anderen Benutzer oder das Programm (auf Basis geplanter Aktionen) hinzugefügt, gelöscht oder modifiziert werden. Verwenden Sie die Schaltfläche **Aktualisieren**, um die Liste der Archive neu aufzubauen.

1. Klicken Sie auf **OK**.

8.1.4 Anmeldedaten der Quelle

Spezifizieren Sie die Anmeldedaten, die für den Zugriff auf den Ort notwendig sind, an dem das Backup-Archiv gespeichert ist.

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Anmeldedaten des Tasks benutzen**

Die Software greift auf den Speicherort mit den Anmeldedaten des Task-Kontos zu, wie sie im Abschnitt **Task-Parameter** spezifiziert wurden.

- **Folgende Anmeldedaten verwenden**

  Die Software greift auf den Speicherort unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu. Verwenden Sie diese Option, wenn das Konto des Tasks keine Zugriffserlaubnis für den Speicherort hat. Es ist möglich, dass Sie für eine Netzwerkfreigabe oder ein Storage Node-Depot noch weitere Anmeldedaten brauchen.

  Spezifizieren Sie:

  - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
  - **Kennwort**. Das Kennwort für das Konto.

2. Klicken Sie auf **OK**.

Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

8.1.5 Validierungszeitpunkt

Da eine Validierung eine Ressourcen-intensive Aktion ist, empfiehlt es sich, sie so zu planen, dass sie nicht zu Hauptbelastungszeiten der verwalteten Maschine erfolgt. Bevorzugen Sie es dagegen, sofort informiert zu werden, ob die gesicherten Daten intakt und daher erfolgreich wiederherstellbar sind, so sollten Sie erwägen, die Validierung direkt nach der Task-Erstellung zu starten.

Wählen Sie eine der folgenden Optionen:

- **Jetzt** – um den Validierungs-Tasks direkt nach seiner Erstellung zu starten, sobald Sie also auf der Validierungs-Seite auf OK geklickt haben.
- **Später** – um einen einmaligen Validierungs-Task zu starten, zu dem von Ihnen angegeben Datum/Zeitpunkt.

  Spezifizieren Sie die passenden Parameter wie folgt:

  - **Datum und Zeit** – das Datum und die Uhrzeit, wann der Task gestartet werden soll.
  - **Task wird manuell gestartet (keine Planung)** – aktivieren Sie dieses Kontrollkästchen, falls Sie den Task später manuell starten wollen.
- **Nach Planung** – um den Task zu planen. Um mehr über die Konfiguration der Planungs-Parameter zu lernen, schauen Sie in den Abschnitt Planung (S. 89).

8.1.6 Anmeldedaten für den Task

Stellen Sie die Anmeldedaten für das Konto zur Verfügung, mit dem der Task ausgeführt wird.

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Unter dem aktuellen Benutzer ausführen**

     Der Task wird mit den Anmeldedaten des Benutzers ausgeführt, der die Tasks startet. Wenn der Task nach Zeit-/Ereignis-Planung laufen soll, werden Sie bei Abschluss der Task-Erstellung nach dem Passwort des aktuellen Benutzers gefragt.
   - **Folgende Anmeldedaten verwenden**

Der Task wird immer mit den von Ihnen spezifizierten Anmeldedaten ausgeführt, egal ob manuell oder per Zeit-/Ereignis-Planung gestartet.

Spezifizieren Sie:

- **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
- **Kennwort**. Das Kennwort für das Konto.

2. Klicken Sie auf **OK**.

Zu weiteren Informationen über die Verwendung von Anmeldedaten in Acronis Backup & Recovery 11.5 siehe den Abschnitt Besitzer und Anmeldedaten (S. 35).

Siehe den Abschnitt 'Benutzerberechtigungen auf einer verwalteten Maschine (S. 37)', um mehr über Aktionen zu erfahren, die in Abhängigkeit von Benutzerberechtigungen verfügbar sind.

8.2 Archive und Backups exportieren

Beim Export wird eine Kopie des Archivs bzw. eine unabhängige Teilkopie des Archivs am von Ihnen angegebenen Speicherort erstellt. Das ursprüngliche Archiv bleibt unverändert.

Ein Export ist möglich für:

- **Ein einzelnes Archiv** – es wird eine exakte Kopie des Archivs erstellt
- **Ein einzelnes Backup** – es wird ein Archiv erstellt, das aus einem einzelnen vollständigen Backup besteht. Beim Export eines inkrementellen oder differentiellen Backups werden die vorhergehenden Backups bis hin zum letzten vollständigen Backup konsolidiert.
- **Ihre Auswahl von Backups**, die zu demselben Archiv gehören – das resultierende Archiv enthält nur die spezifizierten Backups. Eine Konsolidierung erfolgt nach Bedarf; das resultierende Archiv kann daher Voll-Backups enthalten, aber auch inkrementelle und differentielle Backups.
- **Ein komplettes Depot**, das über die Befehlszeilenschnittstelle exportiert werden kann. Weitere Informationen finden Sie in der Acronis Backup & Recovery 11.5 Befehlszeilen-Referenz.

Einsatzszenarien

Mit einem Export können Sie ausgewählte Backups von einer Reihe inkrementeller Backups trennen, um so die Wiederherstellung zu beschleunigen, auf Wechselmedien und externe Medien zu schreiben, oder für andere Zwecke.

Beispiel. Wenn Sie Daten zu einem Remote-Speicherort über eine instabile Netzwerkverbindung oder bei niedriger Netzwerkbandbreite übertragen (etwa ein Backup durch ein WAN unter Verwendung eines VPN-Zugriffs), dann können Sie das anfängliche Voll-Backup auch auf ein Wechselmedium speichern. Schicken Sie das Medium danach zu dem Remote-Speicherort. Dort wird das Backup dann von diesem Medium zu dem als eigentliches Ziel fungierenden Storage exportiert. Nachfolgende inkrementelle Backups, die üblicherweise deutlich kleiner sind, werden dann per Netzwerk/Internet übertragen.

Beim Export eines verwalteten Depots auf ein Wechselmedium erhalten Sie ein transportierbares, nicht verwaltetes Depot für den Einsatz in folgenden Szenarien:

- Aufbewahrung einer externen Kopie (offsite) Ihres Depots oder der wichtigsten Archive.
- 'Physischer' Transport eines Depots zu einer entfernten Niederlassung.
- Wiederherstellung ohne Zugriff auf den Storage Node bei Netzwerkproblemen oder Ausfall des Storage Nodes.

- Wiederherstellung des Storage Node selbst.

Der Export von einem Festplatten-basierten Depot auf ein Bandgerät kann als einfache Form des 'Archiv-Staging' angesehen werden.

Der Name des resultierenden Archivs

Standardmäßig erbt das exportierte Archiv den Namen des ursprünglichen Archivs. Da es nicht empfehlenswert ist, mehrere Archive mit gleichem Namen an einem Ort zu speichern, sind folgende Aktionen bei Verwendung des vorgegebenen Archivnamens deaktiviert:

- Export von Teilen eines Archivs zum selben Speicherort.
- Export eines Archivs oder von Teilen eines Archivs zu einem Speicherort, an dem es ein Archiv mit demselben Namen gibt.
- Zweimaliger Export eines Archivs oder von Teilen eines Archivs zum selben Speicherort.

Wählen Sie in allen genannten Fällen einen Archivnamen, der im Zielordner oder dem Zieldepot nicht vergeben ist. Wenn Sie den Export unter Verwendung desselben Namens erneut ausführen müssen, löschen Sie zunächst das aus dem vorhergehenden Export resultierende Archiv.

Die Optionen des resultierenden Archivs

Das exportierte Archiv erbt die Optionen des ursprünglichen Archivs einschließlich Verschlüsselung und Kennwort. Beim Export eines kennwortgeschützten Archivs werden Sie zur Eingabe des Kennworts aufgefordert. Wenn das ursprüngliche Archiv verschlüsselt ist, wird mit dem Kennwort auch das resultierende Archiv verschlüsselt.

Speicherort für Quelle und Ziel

Wenn die Konsole mit einer **verwalteten Maschine** verbunden ist, können Sie Exports von Archiven oder Teilen eines Archivs von und zu jedem beliebigen Speicherort durchführen, auf den der auf der Maschine befindliche Agent Zugriff hat. Dazu gehören persönliche Depots, lokal angeschlossene Bandgeräte, Wechselmedien und, in den Advanced Editionen, verwaltete und nicht verwaltete zentrale Depots.

Wenn die Konsole mit einem **Management Server** verbunden ist, stehen zwei Exportmethoden zur Verfügung:

- Export aus einem **verwalteten Depot**. Der Export wird vom Storage Node übernommen, der das Depot verwaltet. Das Ziel kann eine Netzwerkfreigabe oder ein lokaler Ordner auf dem Storage Node sein.
- Export aus einem **zentralen, nicht verwalteten Depot**. Der Export wird vom Agenten übernommen, der auf der angegebenen verwalteten Maschine installiert ist. Das Ziel kann jeder Speicherort sein, auf den der Agent Zugriff hat, einschließlich eines verwalteten Depots.

Tipp: *Wählen Sie bei der Konfiguration eines Exports in ein deduplizierendes, verwaltetes Depot eine Maschine, auf der der Deduplizierungs-Add-on für den Agenten installiert ist. Anderenfalls wird der Export-Task fehlschlagen.*

Aktionen mit einem Export-Task

Ein Export-Task startet sofort, nachdem die Konfiguration abgeschlossen ist. Sie können einen Export-Task wie jeden anderen Task stoppen oder löschen.

Sobald ein Export-Task abgeschlossen wurde, können Sie ihn jederzeit erneut ausführen. Löschen Sie zunächst das aus der letzten Ausführung des Task resultierende Archiv, falls es sich noch im Zieldepot

befindet. Anderenfalls wird der Task fehlschlagen. Sie können bei einem Export-Task das Zielarchiv nicht umbenennen (das ist eine Einschränkung).

Tipp: *Dieses Staging-Szenario kann manuell umgesetzt werden, indem Sie immer erst den Task zum Löschen des Archivs und dann den Export-Task ausführen.*

Verschiedene Varianten, einen Export-Task zu erstellen

Gewöhnlich werden Export-Tasks über die Seite **Exportieren** erstellt. Dort können Sie jedes Backup oder Archiv exportieren, auf das Sie Zugriffsrechte besitzen.

Auf die Seite **Exportieren** können Sie aus der Ansicht **Depots** zugreifen. Klicken Sie mit der rechten Maustaste auf das zu exportierende Objekt (Archiv oder Backup) und wählen Sie im Kontextmenü **Exportieren**.

Wählen Sie zuerst ein Validierungsobjekt aus, um Zugriff auf die Seite **Exportieren** zu erhalten: ein Archiv oder ein Backup.

1. Wählen Sie ein Depot. Klicken Sie dazu im Fensterbereich **Navigation** auf das Symbol **Depots** und wählen Sie dann das Depot, indem Sie den Depot-Verzeichnisbaum in der Ansicht **Depots** erweitern oder es direkt im Fensterbereich **Navigation** auswählen.
2. Wählen Sie zur Auswahl eines Archivs zuerst ein Depot an und dann in der Ansicht **Depot** die Registerlasche **Archiv-Anzeige** – anschließend klicken Sie auf den Namen des entsprechenden Archivs.
3. Wählen Sie zur Wahl eines Backups zuerst ein Archiv aus der **Archiv-Anzeige**, erweitern Sie dann das Archiv über die entsprechende Schaltfläche links neben dem Archivnamen und klicken Sie abschließend auf das gewünschte Backup.

Klicken Sie nach Wahl des Validierungsobjektes im Kontextmenü auf den Befehl **Exportieren**. Darauf öffnet sich die Seite **Exportieren** mit dem vorausgewählten Objekt als Quelle. Sie müssen dann nur noch einen Ziel-Speicherort wählen und (optional) einen Namen für den Task angeben.

Führen Sie folgende Schritte aus, um ein Archiv oder ein Backup zu exportieren.

Export-Quelle

Exportieren

Wählen Sie den Typ der zu exportierenden Objekte:

Archiv – in diesem Fall müssen Sie nur das benötigte Archiv spezifizieren.

Backups – Sie müssen zuerst das Archiv spezifizieren und erst danach wählen Sie das/die gewünschten Backup(s) in diesem Archiv.

Durchsuchen

Wählen Sie das **Archiv** (S. 273) oder die **Backups** (S. 273).

Anmeldedaten anzeigen (S. 273)

[Optional] Stellen Sie Anmeldedaten für die Quelle zur Verfügung, falls das Benutzerkonto des Tasks dafür nicht genügend Zugriffsrechte hat.

Export-Ziel

Durchsuchen (S. 274)

Spezifizieren Sie den Pfad zu dem Speicherort, wo das neue Archiv erstellt wird.

Vergeben Sie einen eindeutigen Namen und Kommentar für das neue Archiv.

Vollständige Katalogisierung/Schnelle Katalogisierung

Nicht verfügbar bei bootfähigen Medien oder bei Speicherorten, die keine Katalogisierung unterstützen.

Bestimmen Sie, ob auf die exportierten Backups eine vollständige oder schnelle Katalogisierung durchgeführt werden soll. Weitere Informationen zur Katalogisierung finden Sie im Abschnitt 'Backup-Katalogisierung (S. 119)'.

Anmeldedaten anzeigen (S. 275)

[Optional] Stellen Sie Anmeldedaten für den Ziel-Speicherort zur Verfügung, falls das Benutzerkonto des Tasks nicht ausreichende Zugriffsrechte darauf hat.

Nachdem Sie alle notwendigen Schritte durchgeführt haben, klicken Sie auf **OK**, um den Export zu starten.

Als Ergebnis zeigt das Programm das **Ausführungsstadium** des Tasks in der Ansicht **Backup-Pläne und Tasks** an. Wenn der Task endet, wird im Fenster **Task-Information** das finale Stadium der Task-Ausführung angezeigt.

8.2.1 Auswahl des Archivs

So spezifizieren Sie ein zu exportierendes Archiv

1. Tragen Sie den vollständigen Pfad zum Archiv-Speicherort in das Feld **Pfad** ein – oder wählen Sie den gewünschten Speicherort aus dem Verzeichnisbaum (S. 149).

   Für den Management Server: Wählen Sie im Verzeichnisbaum das verwaltete Depot aus.

2. Wählen Sie das Archiv in der Tabelle rechts vom Verzeichnisbaum. Die Tabelle zeigt die Namen der Archive, die sich in jedem von Ihnen gewählten Speicherort befinden.

   Während Sie den Inhalt eines Speicherorts untersuchen, können Archive durch einen anderen Benutzer oder das Programm (auf Basis geplanter Aktionen) hinzugefügt, gelöscht oder modifiziert werden. Verwenden Sie die Schaltfläche **Aktualisieren**, um die Liste der Archive neu aufzubauen.

3. Klicken Sie auf **OK**.

8.2.2 Auswahl der Backups

So wählen Sie ein zu exportierendes Backup aus

1. Aktivieren Sie oben im Fenster das bzw. die entsprechende(n) Kontrollkästchen.

   Um sicherzugehen, dass Sie das richtige Backup ausgewählt haben, klicken Sie auf das Backup; die untere Tabelle zeigt die in diesem Backup enthaltenen Volumes an.

   Um mehr Informationen über ein Volume zu erhalten, klicken Sie mit der rechten Maustaste darauf und wählen Sie im Kontextmenü **Informationen**.

2. Klicken Sie auf **OK**.

8.2.3 Anmeldedaten der Quelle

Spezifizieren Sie die Anmeldedaten, die für einen Zugriff auf den Ort notwendig sind, an dem das Quellarchiv oder das Backup gespeichert ist.

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:

   - **Aktuelle Anmeldedaten verwenden**

     Die Software greift auf den Speicherort unter Verwendung der Anmeldedaten des aktuellen Benutzers zu.

- **Folgende Anmeldedaten verwenden**

  Das Programm greift auf den Speicherort unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu. Verwenden Sie diese Option, wenn das Konto des Tasks keine Zugriffserlaubnis für den Speicherort hat. Es ist möglich, dass Sie für eine Netzwerkfreigabe oder ein Storage Node-Depot noch weitere Anmeldedaten brauchen.

  Spezifizieren Sie:

  - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
  - **Kennwort**. Das Kennwort für das Konto.

2. Klicken Sie auf **OK**.

Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

8.2.4 Speicherziel wählen

Spezifizieren Sie das Ziel, wohin das exportierte Objekt gespeichert werden soll. Backups dürfen nicht in dasselbe Archiv exportiert werden.

1. Exportziel wählen

Tragen Sie den vollständigen Pfad zum Zielort in das Feld **Pfad** ein oder wählen Sie das gewünschte Ziel im Verzeichnisbaum aus.

- Um Daten in ein zentrales, nicht verwaltetes Depot zu exportieren, erweitern Sie die Gruppe **Zentrale Depots** und wählen dort ein Depot.
- Um Daten in ein persönliches Depot zu exportieren, erweitern Sie die Gruppe **Persönliche Depots** und wählen dort ein Depot.
- Um Daten in einen lokalen Ordner auf der Maschine zu exportieren, erweitern Sie die Gruppe **Lokale Ordner** und wählen das gewünschte Verzeichnis.
- Um Daten zu einer Netzwerkfreigabe zu exportieren, erweitern Sie die Gruppe **Netzwerkordner**, wählen die benötigte Netzwerk-Maschine und klicken dann auf den freigegebenen Ordner. Werden Anmeldedaten zum Zugriff auf die Netzwerkfreigabe benötigt, so wird das Programm diese erfragen.

  ***Hinweis für Linux-Benutzer**: Um eine CIFS-Netzwerkfreigabe (Common Internet File System) anzugeben, die an einen Mount-Punkt wie z.B. /mnt/share angeschlossen ist, wählen Sie diesen Mount-Punkt statt der Netzwerkfreigabe aus.*

- Zum Datenexport auf einen **FTP**- oder **SFTP**-Server tragen Sie Server-Namen oder -Adresse folgendermaßen in das Feld **Pfad** ein:

  ftp://ftp-server:port-nummer oder **sftp://sftp-server:port-nummer**

  Wenn Sie die Port-Nummer nicht angeben, wird Port 21 für FTP benutzt und Port 22 für SFTP.

  Nach Eingabe der Anmeldedaten sind die Ordner auf dem Server verfügbar. Klicken Sie auf den passenden Ordner auf dem Server.

  Sie können auf den Server auch als anonymer Benutzer zugreifen, wenn der Server einen solchen Zugang ermöglicht. Dafür klicken Sie auf **Anonymen Zugang benutzen** anstelle der Eingabe von Anmeldedaten.

Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Klartext über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Packet-Sniffer abgefangen werden.

- Um Daten auf ein lokal angeschlossenes Bandgerät zu exportieren, erweitern Sie die Gruppe **Bandlaufwerke** und klicken auf das benötigte Gerät. In den Standalone-Editionen von Acronis Backup & Recovery 11.5 stehen Bandgeräte nur zur Verfügung, wenn Sie ein Upgrade von Acronis Backup & Recovery 10 durchgeführt haben. Zu weiteren Informationen über die Verwendung von Bändern siehe den Abschnitt 'Bandgerдte (S. 223).

Für den Management Server enthält der Verzeichnisbaum:

- Die Gruppe 'Lokale Ordner', zum Datenexport auf für den Storage Node lokal verfügbare Laufwerke.
- Die Gruppe 'Netzwerkordner', zum Datenexport auf eine Netzwerkfreigabe. Werden Anmeldedaten zum Zugriff auf die Netzwerkfreigabe benötigt, so wird das Programm diese erfragen.

  Hinweis für Linux-Benutzer: Um eine CIFS-Netzwerkfreigabe (Common Internet File System) anzugeben, die an einen Mount-Punkt wie z.B. /mnt/share angeschlossen ist, wählen Sie diesen Mount-Punkt statt der Netzwerkfreigabe aus.

2. Archiv-Tabelle verwenden

Die rechte Tabelle zeigt für jeden im Baum gewählten Speicherort die Namen der dort enthaltenen Archive an, um Ihnen die Wahl des richtigen Ziels zu erleichtern.

Während Sie den Inhalt eines Speicherorts untersuchen, können Archive durch einen anderen Benutzer oder das Programm (auf Basis geplanter Aktionen) hinzugefügt, gelöscht oder modifiziert werden. Verwenden Sie die Schaltfläche **Aktualisieren**, um die Liste der Archive neu aufzubauen.

3. Das neue Archiv benennen

Standardmäßig erbt das exportierte Archiv den Namen des ursprünglichen Archivs. Da es nicht empfehlenswert ist, mehrere Archive mit gleichem Namen an einem Ort zu speichern, sind folgende Aktionen bei Verwendung des vorgegebenen Archivnamens deaktiviert:

- Export von Teilen eines Archivs zum selben Speicherort.
- Export eines Archivs oder von Teilen eines Archivs zu einem Speicherort, an dem es ein Archiv mit demselben Namen gibt.
- Zweimaliger Export eines Archivs oder von Teilen eines Archivs zum selben Speicherort.

Wählen Sie in allen genannten Fällen einen Archivnamen, der im Zielordner oder dem Zieldepot nicht vergeben ist. Wenn Sie den Export unter Verwendung desselben Namens erneut ausführen müssen, löschen Sie zunächst das aus dem vorhergehenden Export resultierende Archiv.

8.2.5 Anmeldedaten für das Ziel

Spezifizieren Sie die Anmeldedaten, die für den Zugriff auf den Ort notwendig sind, an dem das resultierende Archiv gespeichert wird. Der Benutzer, dessen Name angegeben wird, wird als Besitzer des Archivs betrachtet.

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Aktuelle Anmeldedaten verwenden**

Die Software greift auf den Zielort unter Verwendung der Anmeldedaten des aktuellen Benutzers zu.

- **Folgende Anmeldedaten verwenden**

  Die Software greift auf den Zielort unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu. Verwenden Sie diese Option, sofern das Konto des Tasks keine Zugriffserlaubnis für den Zielort hat.

  Spezifizieren Sie:

  - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
  - **Kennwort**. Das Kennwort für das Konto.

2. Klicken Sie auf **OK**.

Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

8.3 Ein Image mounten

Indem Sie die Volumes eines Laufwerk-Backups (Images) mounten, können Sie auf diese Volumes so zugreifen, als wären es physikalische Laufwerke. Wenn mehrere Volumes im selben Backup enthalten sind, dann können Sie diese in einer einzigen Mount-Aktion gleichzeitig anschließen. Die Mount-Aktion ist verfügbar, wenn die Konsole mit einer verwalteten, unter Windows oder Linux laufenden Maschine verbunden ist.

Ein Anschließen der Partitionen im 'Lese/Schreib'-Modus erlaubt Ihnen, den Backup-Inhalt zu modifizieren, d.h. Dateien und Ordner zu speichern, zu verschieben, zu erstellen oder zu löschen und aus einer Datei bestehende, ausführbare Programme zu starten. Die Software erstellt in diesem Modus ein inkrementelles Backup, welches alle Änderungen enthält, die Sie am Backup-Inhalt durchführen. Beachten Sie, dass keine der nachfolgenden Backups diese Änderungen enthalten werden.

Sie können Volumes mounten, falls das Laufwerk-Backup in einem lokalen Ordner (ausgenommen optische Medien), in der Acronis Secure Zone oder auf einer Netzwerkfreigabe gespeichert vorliegt.

Einsatzszenarien

- **Freigeben**: gemountete Images können für Benutzer des Netzwerkes einfach freigegeben werden.
- **Notlösung zur Datenbankwiederherstellung**: mounten Sie ein Image, das eine SQL-Datenbank von einer kürzlich ausgefallenen Maschine enthält. Auf diese Weise erhalten Sie Zugriff auf die Datenbank, bis die ausgefallene Maschine wiederhergestellt ist.
- **Offline Virus-Bereinigung**: wenn eine Maschine befallen ist, fährt der Administrator diese herunter, startet mit einem bootfähigen Medium und erstellt ein Image. Danach mountet der Administrator dieses Image im 'Lese/Schreib'-Modus, scannt und bereinigt es mit einem Antivirus-Programm und stellt schließlich die Maschine wieder her.
- **Fehlerüberprüfung**: Wenn eine Wiederherstellung durch einen Laufwerksfehler fehlschlägt, mounten Sie das Image im 'Lese/Schreib'-Modus. Überprüfen Sie dann das gemountete Laufwerk mit dem Befehl **chkdsk /r**.

Führen Sie folgende Schritte aus, um ein Image zu mounten.

Quelle

Archiv (S. 277)

Spezifizieren Sie den Pfad zum Speicherort des Archivs und wählen Sie die in diesem enthaltenen Laufwerk-Backups.

Backup (S. 278)

Wählen Sie das Backup.

Anmeldedaten (S. 278)

[Optional] Geben Sie die Anmeldeinformationen für den Speicherort des Archivs an.

Mount-Einstellungen

Volumes (S. 278)

Bestimmen Sie die anzuschließenden Partitionen und konfigurieren Sie die Mount-Einstellungen für jedes Laufwerk: Weisen Sie einen Laufwerksbuchstaben zu oder geben Sie den Mount-Punkt an, entscheiden Sie sich dann für den Lese-/Schreib- oder Nur-Lese-Zugriffsmodus.

Nachdem Sie alle benötigten Schritte abgeschlossen haben, klicken Sie auf **OK**, um die Partitionen zu mounten.

8.3.1 Auswahl des Archivs

So wählen Sie ein Archiv aus

1. Geben Sie den vollständigen Pfad zum Speicherort in das Feld **Pfad** ein oder wählen Sie den gewünschten Ort aus dem Verzeichnisbaum:
   - Sollte das Archiv in einem persönlichen Depot gespeichert sein, welches sich in einem lokalen Ordner, in der Acronis Secure Zone oder einer Netzwerkfreigabe befindet, dann erweitern Sie die Gruppe **Persönlich** und klicken Sie auf das benötigte Depot.
   - Wenn das Archiv in einem lokalen Ordner auf der Maschine gespeichert ist, erweitern Sie die Gruppe **Lokale Ordner** und wählen Sie das gewünschte Verzeichnis.

     Die Möglichkeit zum Mounten ist nicht verfügbar, falls das Archiv auf optischen Medien wie CDs, DVDs oder Blu-ray-Medien (BD) gespeichert ist.
   - Falls das Archiv auf einer Netzwerkfreigabe gespeichert ist, dann erweitern Sie die Gruppe **Netzwerkordner**, wählen Sie die gewünschte Netzwerk-Maschine und klicken Sie dann auf den freigegebenen Ordner. Werden Anmeldedaten zum Zugriff auf die Netzwerkfreigabe benötigt, so wird das Programm diese erfragen.

     Hinweis für Linux-Benutzer: *Um eine CIFS-Netzwerkfreigabe (Common Internet File System) anzugeben, die an einen Mount-Punkt (etwa /mnt/share) angeschlossen ist, wählen Sie diesen Mount-Punkt statt der Netzwerkfreigabe aus.*
   - Falls das Archiv in einer NFS-Freigabe gespeichert ist, dann erweitern Sie die Gruppe **NFS-Laufwerke** und klicken Sie auf den entsprechenden Ordner.

     Die Zugriffsmöglichkeit auf NFS-Laufwerke ist nur unter Linux und Linux-basierten bootfähigen Medien verfügbar.
2. Wählen Sie das Archiv in der Tabelle rechts vom Verzeichnisbaum. Die Tabelle zeigt die Namen der Archive, die im gewählten Depot bzw. Ordner enthalten sind.

   Während Sie den Inhalt eines Speicherorts untersuchen, können Archive durch einen anderen Benutzer oder das Programm (auf Basis geplanter Aktionen) hinzugefügt, gelöscht oder

modifiziert werden. Verwenden Sie die Schaltfläche **Aktualisieren**, um die Liste der Archive neu aufzubauen.

3. Klicken Sie auf **OK**.

8.3.2 Auswahl der Backups

So wählen Sie ein Backup aus:

1. Bestimmen Sie eines der Backups anhand seines Zeitstempels.
2. Die untere Tabelle zeigt zur Unterstützung bei der Wahl des richtigen Backups die in diesem Backup enthaltenen Partitionen an.

   Um mehr Informationen über ein Laufwerk zu erhalten, klicken Sie mit der rechten Maustaste darauf und wählen im Kontextmenü **Informationen**.
3. Klicken Sie auf **OK**.

8.3.3 Anmeldedaten

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Aktuelle Anmeldedaten verwenden**

     Das Programm greift auf den Speicherort unter Verwendung der Anmeldedaten des aktuellen Benutzers zu.
   - **Folgende Anmeldedaten verwenden**

     Das Programm greift auf den Speicherort unter Verwendung der von Ihnen spezifizierten Anmeldedaten zu. Verwenden Sie diese Option, sofern das aktuelle Benutzerkonto keine Zugriffserlaubnis für den Speicherort hat. Es ist möglich, dass Sie für eine Netzwerkfreigabe oder ein Storage Node-Depot noch weitere Anmeldedaten brauchen.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
2. Klicken Sie auf **OK**.

Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Plain-Text über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Paket-Sniffer abgefangen werden.

8.3.4 Auswahl der Partition

Bestimmen Sie die anzuschließenden Partitionen und konfigurieren Sie die Parameter zum Mounten für jedes der gewählten Laufwerke wie folgt:

1. Aktivieren Sie das Kontrollkästchen für jede Partition, die Sie mounten müssen.
2. Klicken Sie auf das gewählte Laufwerk, um die Parameter zum Mounten einzustellen.
   - **Zugriffsmodus** – bestimmen Sie den Modus, mit dem Sie das Laufwerk anschließen wollen:
     - **Nur Lesen** – ermöglicht Ihnen das Durchsuchen und Öffnen von Dateien innerhalb des Backups, ohne dass es zu irgendwelchen Änderungen kommen kann.

        - **Lesen/Schreiben** – in diesem Modus geht das Programm davon aus, dass der Backup-Inhalt verändert wird, und erstellt ein inkrementelles Backup, um diese Veränderungen aufzunehmen.
    - **Laufwerksbuchstabe zuweisen** (in Windows) – Acronis Backup & Recovery 11.5 wird dem angeschlossenen Laufwerk einen freien Laufwerksbuchstaben zuweisen. Wählen Sie sofern benötigt aus dem Listenfeld einen anderen Laufwerksbuchstaben.
    - **Mount-Punkt** (in Linux) – spezifiziert das Verzeichnis, wo Sie die Partition gemountet haben wollen.
3. Sollten mehrere Partitionen zum Anschließen ausgewählt sein, so klicken Sie auf jedes Laufwerk, um wie im vorherigen Schritt beschrieben die Parameter zum Mounten einzustellen.
4. Klicken Sie auf **OK**.

8.3.5 Gemountete Images verwalten

Sobald eine Partition angeschlossen wurde, können Sie im Backup enthaltene Dateien und Ordner mit einem Datei-Manager durchsuchen und gewünschte Dateien zu einem beliebigen Ziel kopieren. Sie müssen daher keine vollständige Wiederherstellungsprozedur durchführen, wenn Sie nur einige Dateien und Ordner aus einem Partitions-Backup entnehmen müssen.

Images durchsuchen

Über das Durchsuchen von angeschlossenen Partitionen können Sie den Laufwerksinhalt einsehen und auch modifizieren (sofern im Lese-/Schreib-Modus gemountet).

Um eine angeschlossene Partition zu durchsuchen, wählen Sie das Laufwerk in der Tabelle aus und klicken auf **Durchsuchen**. Darauf öffnet sich das Fenster des Standard-Datei-Managers und erlaubt Ihnen so, den Inhalt des gemounteten Laufwerkes zu untersuchen.

Abbild abschalten

Ein gemountetes Laufwerk im System zu belassen, benötigt einiges an System-Ressourcen. Es ist daher empfehlenswert, dass Sie die Laufwerke, nachdem alle notwendigen Aktionen abgeschlossen wurden, wieder abschalten. Ein Laufwerk bleibt bis zum nächsten Neustart des Betriebssystems gemountet, wenn Sie es nicht manuell abschalten.

Um ein Image abzuschalten, wählen Sie es in der Tabelle aus und klicken dann auf **Abschalten**.

Um alle gemounteten Laufwerke abzuschalten, klicken Sie auf **Alle abschalten**.

8.4 In Depots verfügbare Aktionen

Durch die Verwendung von Depots haben Sie einen einfachen Zugriff auf Archive und Backups und können Sie Archivverwaltungsaktionen ausführen.

So führen Sie Aktionen mit Archiven und Backups aus

1. Wählen Sie im Fensterbereich **Navigation** das Depot aus, dessen Archive Sie verwalten wollen.
2. Wählen Sie in der Ansicht 'Depot' die Registerlasche **Archiv-Anzeige**. Diese Registerlasche zeigt alle in dem gewählten Depot gespeicherten Archive an.
3. Wie Sie fortfahren ist beschrieben unter:
    - Aktionen mit Archiven (S. 280)
    - Aktionen mit Backups (S. 280)

8.4.1 Aktionen mit Archiven

So führen Sie Aktionen mit einem Archiv aus

1. Wählen Sie im Fensterbereich **Navigation** das Depot, welches die Archive enthält.
2. Wählen Sie in der Registerlasche **Archiv-Anzeige** dieses Depots das gewünschte Archiv. Wenn das Archiv mit einem Kennwort geschützt ist, werden Sie aufgefordert, dieses Kennwort einzugeben.
3. Führen Sie Aktionen aus, indem Sie auf die entsprechenden Schaltflächen der Symbolleiste klicken. Sie können auf diese Aktionen auch über das Hauptmenüelement **'[Archivname]' Aktionen** zugreifen.

Nachfolgend finden Sie eine Anleitung zur Durchführung von Aktionen mit Archiven, die in einem Depot gespeichert sind.

Aktion	Lösung
Ein Archiv validieren	Klicken Sie auf **Validieren**. Sie gelangen zur Seite **Validierung** (S. 266) mit dem bereits als Quelle vorausgewählten Archiv. Die Validierung eines Archivs überprüft die Gültigkeit aller Backups im Archiv.
Ein Archiv exportieren	Klicken Sie auf **Exportieren**. Darauf öffnet sich die Seite **Export** (S. 270) mit dem vorausgewählten Archiv als Quelle. Beim Export wird ein Duplikat des Archivs einschließlich aller enthaltenen Backups am von Ihnen angegebenen Speicherort erstellt.
Ein einzelnes oder mehrere Archive löschen	1. Wählen Sie ein oder mehrere Archive, das/die sie löschen wollen. 2. Klicken Sie auf **Löschen**. Das Programm dupliziert Ihre Wahl im Fenster **Backups löschen** (S. 282), wo jedes Archiv bzw. Backup sein eigenes Kontrollkästchen hat. Überprüfen Sie die Auswahl und korrigieren Sie diese, sofern nötig (aktivieren Sie das Kontrollkästchen für ein gewünschtes Archiv), bestätigen Sie danach die Löschaktion.
Alle Archive in einem Depot löschen	Beachten Sie, dass Sie nicht den gesamten Depot-Inhalt sehen, wenn auf die Depot-Liste ein Filter angewendet wurde. Stellen Sie sicher, dass das Depot keine zu bewahrenden Archive enthält, bevor Sie die Aktion starten. Klicken Sie auf **Alle Löschen**. Das Programm dupliziert Ihre Wahl in einem neuen Fenster, welches für jedes Archiv bzw. Backup Kontrollkästchen hat. Überprüfen Sie Ihre Wahl und korrigieren Sie diese falls nötig; bestätigen Sie dann die Löschaktion.

8.4.2 Aktionen mit Backups

So führen Sie beliebige Aktionen mit einem Backup aus

1. Wählen Sie im Fensterbereich **Navigation** das Depot, welches die Archive enthält.
2. Wählen Sie in der Registerlasche **Archiv-Anzeige** dieses Depots das gewünschte Archiv. Erweitern Sie dann das Archiv und klicken Sie auf das Backup, um es auszuwählen. Wenn das Archiv mit einem Kennwort geschützt ist, werden Sie aufgefordert, dieses Kennwort einzugeben.
3. Führen Sie Aktionen aus, indem Sie auf die entsprechenden Schaltflächen der Symbolleiste klicken. Sie können auf diese Aktionen auch über das Hauptmenüelement **'[Backup-Name]' Aktionen** zugreifen.

Nachfolgend finden Sie eine Anleitung zur Durchführung von Aktionen mit Backups.

Aufgabe	Lösung
Backup-Inhalte in einem separaten Fenster einsehen	Klicken Sie auf **Inhalt anzeigen**. Überprüfen Sie im Fenster **Backup-Inhalt** die entsprechend angezeigten Daten.
Recovery	Klicken Sie auf **Recovery**. Sie gelangen zur Seite **Daten wiederherstellen** (S. 146), mit dem bereits als Quelle vorausgewählten Backup.
Ein Laufwerk-/Volume-Backup zu einer virtuellen Maschine konvertieren	Klicken Sie mit der rechten Maustaste auf das Laufwerk-Backup und wählen Sie **Zu VM konvertieren**. Sie gelangen zur Seite **Daten wiederherstellen** (S. 146), mit dem bereits als Quelle vorausgewählten Backup. Wählen Sie Zielort sowie Typ der neuen virtuellen Maschine und fahren Sie dann so wie bei einer regulären Laufwerk- bzw. Volume-Wiederherstellung fort.
Ein Backup validieren	Klicken Sie auf **Validieren**. Sie gelangen zur Seite **Validierung** (S. 266), mit dem bereits als Quelle vorausgewählten Backup. Die Validierung eines Datei-Backups imitiert die Wiederherstellung aller Dateien eines Backups an einen virtuellen Zielort. Die Validierung eines Laufwerk-Backups berechnet eine Prüfsumme für jeden Datenblock, der im Backup gespeichert ist.
Ein Backup exportieren	Klicken Sie auf **Exportieren**. Darauf öffnet sich die Seite **Exportieren** (S. 270) mit dem vorausgewählten Backup als Quelle. Beim Exportieren wird ein neues Archiv mit einer unabhängigen Kopie des Backups an dem von Ihnen angegebenen Speicherort erstellt.
Ein Backup zu einem Voll-Backup konvertieren	Klicken Sie auf **Zu Voll-Backup konvertieren**, um ein inkrementelles oder differentielles Backup durch ein Voll-Backup zu ersetzen, das dem gleichen Backup-Zeitpunkt entspricht. Zu weiteren Informationen siehe den Abschnitt 'Ein Backup zu einem Voll-Backup konvertieren (S. 282)'.
Ein einzelnes oder mehrere Backups löschen	Wählen Sie das gewünschte Backup und klicken Sie dann auf **Löschen**. Das Programm dupliziert Ihre Wahl im Fenster **Backups löschen** (S. 282), wo jedes Archiv bzw. Backup sein eigenes Kontrollkästchen hat. Überprüfen Sie die Auswahl und korrigieren Sie diese, sofern nötig (aktivieren Sie das Kontrollkästchen für ein gewünschtes Backup); bestätigen Sie danach die Löschaktion.
Alle Archive und Backups in einem Depot löschen	Beachten Sie, dass Sie nicht den gesamten Depot-Inhalt sehen, wenn auf die Depot-Liste ein Filter angewendet wurde. Stellen Sie sicher, dass das Depot keine zu bewahrenden Archive enthält, bevor Sie die Aktion starten. Klicken Sie auf **Alle Löschen**. Das Programm dupliziert Ihre Wahl im Fenster **Backups löschen** (S. 282), wo jedes Archiv bzw. Backup sein eigenes Kontrollkästchen hat. Überprüfen Sie Ihre Wahl und korrigieren Sie diese falls nötig; bestätigen Sie dann die Löschaktion.

8.4.3 Ein Backup zu einem Voll-Backup konvertieren

Wenn in einem Archiv die Kette inkrementeller Backups ziemlich lang wird, können Sie die Zuverlässigkeit Ihres Archivs erhöhen, indem Sie ein inkrementelles Backup in ein Voll-Backup konvertieren. Sie können auf Wunsch auch ein differentielles Backup konvertieren, falls es auf diesem beruhende inkrementelle Backups gibt.

Während der Konvertierung wird das gewählte inkrementelle oder differentielle Backup durch ein Voll-Backup ersetzt, das demselben Backup-Zeitpunkt entspricht. Die anderen, vorhergehenden Backups in der Kette werden nicht verändert. Alle nachfolgenden inkrementellen und differentiellen Backups werden bis zum nächsten Voll-Backup ebenfalls aktualisiert. Die neuen Backup-Versionen werden zuerst erstellt und erst danach werden die älteren gelöscht. Der Speicherort muss daher über ausreichend Speicherplatz verfügen, um vorübergehend die alten und neuen Versionen aufnehmen zu können.

Beispiel

Sie haben folgende Backup-Kette in Ihrem Archiv:

```
F1 I2 I3 I4 D5 I6 I7 I8 F9 I10 I11 D12 F13
```

Dabei steht **F** für Voll-Backup (Full), **I** für inkrementell und **D** für differentiell.

Sie konvertieren das **I4**-Backup zu einem Voll-Backup. Die Backups **I4, D5, I6, I7, I8** werden aktualisiert, während **I10 I11 D12** unverändert bleiben, da sie auf **F9** basieren.

Tipps zur Verwendung

Die Konvertierung erstellt keine Kopie eines Backups. Um eine selbstständige Kopie eines Backups auf einem Flash-Laufwerk (USB-Stick) oder Wechselmedium zu erhalten, verwenden Sie die Aktion 'Exportieren (S. 270)'.

Beim Mounten eines Images (S. 276) im 'Lese/Schreib'-Modus erstellt die Software ein inkrementelles Backup, welches alle Änderungen enthält, die Sie am Backup-Inhalt durchführen. Die nachfolgenden Backups werden diese Änderungen nicht enthalten. Falls Sie normalerweise eines der nachfolgenden Backups zu 'vollständig' konvertieren, tauchen keine dieser Änderungen im resultierenden Voll-Backup auf.

Beschränkungen

Für folgende Backups ist keine Konvertierung erlaubt:

- Backups, die auf Bändern, auf CDs/DVDs oder im Acronis Online Backup Storage gespeichert sind.
- Backups, die vereinfachte Namen (S. 83) haben.
- Backups von Microsoft Exchange-Server-Daten.

8.4.4 Archive und Backups löschen

Das Fenster **Backups löschen** zeigt dieselbe Registerlasche wie die Ansicht „Depots“, jedoch mit Kontrollkästchen für jedes Archiv und Backup. Das von Ihnen zum Löschen gewählte Archiv bzw. Backup ist entsprechend markiert. Überprüfen Sie das von Ihnen zum Löschen gewählte Archiv bzw. Backup. Wenn Sie noch weitere Archive und Backups löschen müssen, aktivieren Sie die entsprechenden Kontrollkästchen, klicken dann auf **Ausgewählte löschen** und bestätigen die Löschaktion.

Was passiert, wenn ich ein Backup lösche, das als Basis für ein inkrementelles oder differentielles Backup dient?

Das Programm konsolidiert die beiden Backups, um die Archiv-Konsistenz zu wahren. Ein Beispiel: Sie löschen ein Voll-Backup, behalten aber das nächste inkrementelle. Die Backups werden zu einem einzelnen Voll-Backup kombiniert, welches den Zeitstempel des inkrementellen Backups erhält. Wenn Sie ein inkrementelles oder differentielles Backup aus der Mitte einer Kette löschen, wird der resultierende Backup-Typ inkrementell.

Machen Sie sich bewusst, dass Konsolidierung nur eine Methode, aber keine Alternative zum Löschen ist. Das resultierende Backup wird keine Daten enthalten, die im gelöschten Backup vorlagen, die jedoch im beibehaltenen inkrementellen oder differentiellen Backup fehlten.

Das Depot sollte genügend Speicherplatz für während einer Konsolidierung erstellte temporäre Dateien haben. Aus einer Konsolidierung resultierende Backups sind immer maximal komprimiert.

9 Bootfähiges Medium

Bootfähiges Medium

Ein bootfähiges Medium ist ein physikalisches Medium (CD, DVD, USB-Flash-Laufwerk oder andere Wechselmedien, die vom BIOS einer Maschine als Boot-Gerät unterstützt werden), das auf jeder PC-kompatiblen Maschine startet und es Ihnen ermöglicht, den Acronis Backup & Recovery 11.5 Agenten in einer Linux-basierte Umgebung oder unter Windows Preinstallation Environment (WinPE) auszuführen (also ohne die Hilfe eines bereits vorhandenen Betriebssystems). Bootfähige Medien werden am häufigsten verwendet, um:

- ein Betriebssystem wiederherzustellen, das nicht mehr bootet
- auf Daten zuzugreifen und zu sichern, die in einem beschädigten System überlebt haben
- ein Betriebssystem auf fabrikneue Computer zu verteilen
- Volumes vom Typ 'Basis' oder 'Dynamisch' auf fabrikneuen Geräten einzurichten
- Laufwerke, die ein nicht unterstütztes Dateisystem verwenden, mit einem Sektor-für-Sektor-Backup zu sichern
- Daten 'offline' zu sichern, die wegen einer Zugangsbeschränkung, einer Sperrung durch laufende Anwendungen oder wegen anderer Gründe nicht 'online' gesichert werden können.

Eine Maschine kann in die genannten Umgebungen entweder mit physikalischen Medien oder durch Netzwerk-Booten von einem Acronis PXE Server, von einem Windows Deployment Service (WDS) oder Remote Installation Service (RIS) gestartet werden. Diese Server mit ihren hochgeladenen, bootfähigen Komponenten können auch als eine Art bootfähiger Medien betrachtet werden. Sie können mit demselben Assistenten bootfähige Medien erstellen und den PXE Server oder WDS/RIS-Dienste konfigurieren.

Linux-basiertes bootfähiges Medium

Linux-basierte Medien enthalten einen bootfähigen Acronis Backup & Recovery 11.5 Agenten, der auf einem Linux-Kernel beruht. Der Agent kann auf jeder PC-kompatiblen Hardware booten und dort Aktionen ausführen, einschließlich auf fabrikneuer Hardware und Maschinen mit beschädigten oder nicht unterstützten Dateisystemen. Diese Aktionen können per Management Konsole konfiguriert und gesteuert werden – lokal oder per Remotesteuerung.

PE-basiertes bootfähiges Medium

PE-basierte bootfähige Medien enthalten ein funktionsreduziertes Windows, Windows Preinstallation Environment (WinPE) genannt, sowie ein Acronis Plug-in für WinPE; dabei handelt es sich um eine Modifikation des Acronis Backup & Recovery 11.5 Agenten, damit dieser unter WinPE laufen kann.

WinPE hat sich gerade bei großen IT-Umgebungen mit unterschiedlicher Hardware als sehr praktische bootfähige Lösung erwiesen.

Vorteile:

- Die Verwendung von Acronis Backup & Recovery 11.5 in WinPE bietet mehr Funktionalität als die Verwendung Linux-basierter bootfähiger Medien. Indem Sie Ihre PC-kompatible Hardware mit WinPE booten, können Sie nicht nur den Acronis Backup & Recovery 11.5 Agenten verwenden, sondern auch PE-Befehle, Skripte und andere Plug-ins, die Sie in WinPE eingebunden haben.

- Bootfähige Medien auf PE-Basis helfen, Linux-bezogene Probleme zu umgehen, z.B. fehlende Unterstützung für RAID-Controller oder gewisse RAID-Level. Auf WinPE 2.x (und höher) basierende Medien ermöglichen es, benötigte Gerätetreiber dynamisch zu laden.

Beschränkung:

- Bootfähige Medien, die auf WinPE vor Version 4.0 basieren, können keine Maschinen booten, die UEFI (Unified Extensible Firmware Interface) verwenden.

9.1 So erstellen Sie ein bootfähiges Medium

Acronis bietet Ihnen mit dem Acronis Bootable Media Builder ein spezielles Werkzeug zur Erstellung bootfähiger Medien.

Der Bootable Media Builder erfordert keine Lizenz, wenn er zusammen mit einem Agenten installiert wird. Alle Add-ons für den Agenten stehen, sofern installiert, auch in der Notfallumgebung zur Verfügung. Um einen Media Builder auf einer Maschine ohne Agenten nutzen zu können, müssen Sie einen Lizenzschlüssel eingeben oder wenigstens eine Lizenz auf dem License Server verfügbar haben. Die Lizenz kann entweder verfügbar oder zugewiesen sein.

Um ein physikalisches Medium erzeugen zu können, muss die Maschine über einen CD-/DVD-Brenner verfügen oder ein Flash-Laufwerk (z.B. USB-Stick) anschließbar sein. Um PXE oder WDS/RIS konfigurieren zu können, muss die Maschine eine Netzverbindung haben. Der Bootable Media Builder kann außerdem das ISO-Image einer bootfähigen Disc erstellen, um dieses später auf ein leeres Medium zu brennen.

Nachfolgend finden Sie Anleitungen zur Erstellung bootfähiger Medien.

9.1.1 Linux-basiertes bootfähiges Medium

So erstellen Sie ein Linux-basiertes Boot-Medium

1. Starten Sie den Bootable Media Builder entweder über die Management Konsole durch **Extras –> Bootfähiges Medium erstellen** oder als eigenständige Komponente.
2. Sollte der Agent für Windows oder der Agent für Linux auf der Maschine *nicht installiert* sein, dann spezifizieren einen Lizenzschlüssel oder einen License Server mit seinen Lizenzen. Die Lizenzen werden nicht zugewiesen oder neu zugewiesen. Sie helfen zu bestimmen, welche Funktionen für das erstellte Medium aktiviert werden sollen. Ohne Lizenz können Sie ein Medium erstellen, mit dem Sie nur Wiederherstellungen vom Online Backup Storage durchführen können.

   Sollte der Agent für Windows oder der Agent für Linux auf der Maschine *doch installiert* sein, dann übernimmt das Medium dessen Funktionalität, einschließlich Universal Restore und Deduplizierung.
3. Wählen Sie den **Typ des bootfähigen Mediums: Standard (Linux-basiertes Medium)**.

   Bestimmen Sie, wie Volumes und Netzwerk-Ressourcen gehandhabt werden – den so genannten 'Stil' des Mediums:

   - Ein Medium mit Linux-typischer Volume-Behandlung stellt die Volumes beispielsweise als hda1 und sdb2 dar. Es versucht, MD-Geräte und logische Volumes (vom LVM verwaltet) vor Start einer Wiederherstellung zu rekonstruieren.
   - Ein Medium, das Volumes Windows-typisch behandelt, verwendet Laufwerksbuchstaben zur Darstellung von Volumes, beispielsweise C: und D:. Es bietet Zugriff auf dynamische Volumes (LDM verwaltet).
4. Folgen Sie den Assistentenschritten, um Folgendes zu spezifizieren:

a. [Optional] Parameter für den Linux-Kernel. Trennen Sie mehrere Parameter per Leerzeichen.

   Um beispielsweise bei jedem Start des bootfähigen Agenten einen Anzeigemodus für das Medium auswählen zu können, geben Sie an: **vga=ask**

   Eine Liste der Parameter finden Sie unter 'Kernel-Parameter (S. 286)'.

b. Die Acronis Bootable Components, die das bootfähige Medium später enthalten soll.

   Sie können 32-Bit- und/oder 64-Bit-Komponenten wählen. Die 32-Bit-Komponenten funktionieren auch auf 64-Bit-Hardware. Sie benötigen jedoch 64-Komponenten, um von einer Maschine booten zu können, die UEFI (Unified Extensible Firmware Interface) verwendet.

   Um das Medium auf verschiedenen Hardware-Typen verwenden zu können, wählen Sie beide Komponententypen. Wenn Sie dann eine Maschine mit dem resultierenden Medium booten, können Sie die 32-Bit- oder 64-Bit-Komponenten dann aus dem Boot-Menü auswählen.

c. [Optional] Das Timeout-Intervall für das Boot-Menü, sowie die Komponente, die automatisch nach dem Zeitlimit gestartet wird.

   - Sofern nicht anders konfiguriert, wartet der Acronis Loader auf eine Auswahl, ob das Betriebssystem (sofern vorhanden) oder die Acronis-Komponente gestartet werden soll.
   - Wenn Sie z.B. **10 Sek.** für den bootfähigen Agenten einstellen, wird dieser 10 Sekunden nach Anzeige des Menüs starten. Dies ermöglicht den unbeaufsichtigten Betrieb vor Ort, wenn von einem PXE Server oder WDS/RIS gebootet wird.

d. [Optional] Remote-Anmeldeeinstellungen:

   - Einzugebender Benutzername und Kennwort auf Konsolenseite bei Verbindung zum Agenten. Falls Sie diese Felder leer lassen, wird die Verbindung ohne die Angabe von Anmeldedaten aufgebaut.

e. [Optional] Netzwerkeinstellungen (S. 288):

   - TCP/IP-Einstellungen, die dem Netzwerkadapter der Maschine zugewiesen werden.

f. [Optional] Netzwerk-Port (S. 289):

   - Der TCP-Port, den der bootfähige Agent auf einkommende Verbindungen kontrolliert.

g. Der zu erstellende Medientyp. Sie können:

   - CDs, DVDs oder andere bootfähige Medien erstellen (z.B. USB-Sticks), sofern das BIOS der Hardware das Booten von diesen Medien erlaubt
   - Ein ISO-Image des bootfähigen Mediums erstellen, um es später auf einen leeren Rohling zu brennen
   - Gewählte Komponenten auf den Acronis PXE Server hochladen
   - Die gewählten Komponenten auf einen WDS/RIS hochladen.

h. [Optional] Windows System-Treiber zur Verwendung durch Acronis Universal Restore (S. 289). Dieses Fenster erscheint nur, wenn das Add-on Acronis Universal Restore installiert ist und ein anderes Medium als PXE oder WDS/RIS gewählt wurde.

i. Pfad zur ISO-Datei des Mediums oder Name oder IP-Adresse inklusive Anmeldedaten für den PXE-Server oder WDS/RIS.

9.1.1.1 Kernel-Parameter

In diesem Fenster können Sie einen oder mehrere Parameter des Linux-Kernel angeben. Diese werden automatisch wirksam, wenn das bootfähige Medium startet.

Typischerweise kommen diese Parameter zur Anwendung, wenn während der Arbeit mit bootfähigen Medien Probleme auftauchen. Normalerweise brauchen Sie in dieses Feld nichts einzutragen.

Sie können jeden dieser Parameter auch durch Drücken der Taste F11 im Boot-Menü angeben.

Parameter

Trennen Sie mehrere Parameter mit Leerzeichen.

acpi=off

Deaktiviert ACPI (Advanced Configuration and Power Interface). Dieser Parameter kann hilfreich sein, wenn bei einer bestimmten Hardware-Konfiguration Probleme auftauchen.

noapic

Deaktiviert APIC (Advanced Programmable Interrupt Controller). Dieser Parameter kann hilfreich sein, wenn bei einer bestimmten Hardware-Konfiguration Probleme auftauchen.

vga=ask

Erfragt den Grafikkartenmodus, der in der grafischen Benutzeroberfläche eines bootfähigen Mediums verwendet werden soll. Ist kein **vga**-Parameter angegeben, wird der Videomodus automatisch erkannt.

vga=*mode_number*

Spezifiziert den Grafikkartenmodus, der in der grafischen Benutzeroberfläche des bootfähigen Mediums verwendet werden soll. Die Modus-Nummer wird unter *mode_number* im Hexadezimalformat angegeben, z.B.: **vga=0x318**

Die Bildschirmauflösung und die Anzahl der Farben für eine Modus-Nummer können sich von Maschine zu Maschine unterscheiden. Es wird empfohlen, zunächst den Parameter **vga=ask** zu verwenden, um einen Wert für *mode_number* auszuwählen.

quiet

Deaktiviert die Anzeige von Pop-up-Meldungen während der Linux-Kernel geladen wird und startet danach die Management Konsole.

Dieser Parameter wird implizit bei der Erstellung von bootfähigen Medien spezifiziert; Sie können ihn jedoch im Boot-Menü entfernen.

Wenn der Parameter nicht angegeben ist, werden alle Meldungen beim Start angezeigt, gefolgt von einer Eingabeaufforderung. Geben Sie bei der Eingabeaufforderung folgenden Befehl ein, um die Management Konsole zu starten: **/bin/product**

nousb

Deaktiviert, dass das USB-Subsystem geladen wird.

nousb2

Deaktiviert die USB 2.0-Unterstützung. USB 1.1-Geräte arbeiten, auch wenn dieser Parameter gesetzt ist. Mit dem Parameter können Sie manche USB-Laufwerke im USB 1.1-Modus verwenden, wenn sie im USB 2.0-Modus nicht arbeiten.

nodma

Deaktiviert den Speicherdirektzugriff (DMA) für alle IDE-Festplatten. Verhindert auf mancher Hardware ein Einfrieren des Kernels.

nofw

Deaktiviert die Unterstützung für die FireWire (IEEE1394)-Schnittstelle.

nopcmcia

Deaktiviert die Erkennung von PCMCIA-Hardware.

nomouse

Deaktiviert die Maus-Unterstützung.

module_name=**off**

Deaktiviert das Modul, dessen Name in *module_name* angeben ist. Um beispielsweise die Nutzung des SATA-Moduls zu deaktivieren, geben Sie folgenden Wert an: **sata_sis=off**

pci=bios

Erzwingt die Verwendung des PCI-BIOS statt direkt auf die Hardware-Geräte zuzugreifen. Dieser Parameter kann hilfreich sein, z.B. wenn die Maschine eine nicht standardgemäße PCI Host-Bridge hat.

pci=nobios

Deaktiviert die Verwendung des PCI BIOS und erlaubt nur direkte Hardware-Zugriffsmethoden. Dieser Parameter kann z.B. hilfreich sein, wenn das bootfähige Medium nicht startet und dies wahrscheinlich durch das BIOS verursacht wird.

pci=biosirq

Verwendet PCI BIOS-Aufrufe, um die Interrupt Routing-Tabelle zu erhalten. Dieser Parameter kann hilfreich sein, wenn es dem Kernel nicht gelingt, Unterbrechungsanforderungen (IRQs) zuzuordnen oder den sekundären PCI-Bus auf dem Mainboard zu finden.

Auf einigen Maschinen funktionieren diese Aufrufe möglicherweise nicht richtig. Es kann unter Umständen aber der einzige Weg sein, die Interrupt Routing-Tabelle anzuzeigen.

9.1.1.2 Netzwerk-Einstellungen

Sie erhalten während der Erstellung bootfähiger Acronis-Medien die Möglichkeit, die Netzwerkverbindungen vorzukonfigurieren, die vom bootfähigen Agenten verwendet werden. Die folgenden Parameter können vorkonfiguriert werden:

- IP-Adresse
- Subnetzmaske
- Gateway
- DNS-Server
- WINS-Server

Sobald der bootfähige Agent auf einer Maschine gestartet ist, wird die Konfiguration auf die Netzwerkkarte (NIC) der Maschine angewendet. Wenn die Einstellungen nicht vorkonfiguriert wurden, benutzt der Agent eine DHCP-Autokonfiguration. Sie haben außerdem die Möglichkeit, die Netzwerkeinstellungen manuell vorzunehmen, sobald der bootfähige Agent auf der Maschine läuft.

Mehrfache Netzwerkverbindungen vorkonfigurieren

Sie können die TCP/IP-Einstellungen für bis zu zehn Netzwerkkarten vorkonfigurieren. Um sicherzustellen, dass jede Netzwerkkarte die passenden Einstellungen bekommt, sollten Sie das Medium auf dem Server erstellen, für den das Medium konfiguriert wird. Wenn Sie eine existierende NIC im Assistentenfenster anwählen, werden ihre Einstellungen zur Speicherung auf das Medium übernommen. Die MAC-Adresse jeder existierenden NIC wird ebenso auf dem Medium gespeichert.

Sie können die Einstellungen ändern, mit Ausnahme der MAC-Adresse; oder Einstellungen für nicht existierende NICs konfigurieren, falls das nötig ist.

Sobald der bootfähige Agent auf dem Server gestartet ist, fragt er die Liste der verfügbaren NICs ab. Diese Liste ist nach den Steckplätzen sortiert, die von den NICs belegt werden. An der Spitze stehen die, die dem Prozessor am nächsten liegen.

Der bootfähige Agent teilt jeder bekannten NIC die passenden Einstellungen zu, wobei die NICs anhand ihrer MAC-Adressen identifiziert werden. Nachdem die NICs mit bekannten MAC-Adressen konfiguriert wurden, bekommen die verbliebenen NICs (beginnend mit der untersten in der Liste) die Einstellungen zugewiesen, die Sie für unbekannte NICs vorkonfiguriert haben.

Sie können bootfähige Medien für jede beliebige Maschine konfigurieren – und nicht nur für die Maschine, auf der das Medium erstellt wurde. Um dies durchzuführen, konfigurieren Sie die NICs entsprechend ihrer Steckplatzreihenfolge in der betreffenden Maschine. NIC1 besetzt den zum Prozessor am nächsten liegenden Steckplatz, NIC2 wiederum den folgenden und so weiter. Wenn der bootfähige Agent auf der Maschine startet, wird er keine NICs mit bekannter MAC-Adresse finden und daher die NICs in der von Ihnen bestimmten Reihenfolge konfigurieren.

Beispiel

Der bootfähige Agent könnte einen der Netzwerkadapter zur Kommunikation mit der Management Konsole innerhalb des Fertigungsnetzwerkes nutzen. Für diese Verbindung könnte eine automatische Konfiguration durchgeführt werden. Größere Datenmengen für eine Wiederherstellung könnten über die zweite NIC übertragen werden, die in das dafür bestimmte Backup-Netzwerk mit Hilfe statischer TCP/IP-Einstellungen eingebunden ist.

9.1.1.3 Netzwerk-Port

Bei der Erstellung bootfähiger Medien finden Sie eine Option zur Vorkonfiguration des Netzwerk-Ports, auf dem der bootfähige Agent nach einkommenden Verbindungen horcht. Es besteht die Wahl zwischen:

- dem Standard-Port
- dem aktuell verwendeten Port
- dem neuen Port (geben Sie die Port-Nummer ein)

Sofern der Port nicht vorkonfiguriert wurde, verwendet der Agent die Standard-Port-Nummer (9876). Dieser Port wird außerdem auch als Standard von der Acronis Backup & Recovery 11.5 Management Console verwendet.

9.1.1.4 Treiber für Universal Restore

Während der Erstellung der bootfähigen Medien erhalten Sie eine Option, um Windows-Treiber dem Medium hinzuzufügen. Diese Treiber werden von Universal Restore verwendet, sofern Windows auf einer Maschine wiederhergestellt wird, die im Bezug zum ursprünglichen Backup-System beim Prozessor, Mainboard oder Massenspeichergeräten abweicht.

Sie können Universal Restore auch konfigurieren:

- um das Medium nach Treibern zu durchsuchen, die auf die Ziel-Hardware am besten passen
- um die Massenspeicher-Treiber einzubinden, die Sie ausdrücklich vom Medium aus spezifiziert haben. Dies ist notwendig, wenn die Ziel-Hardware einen spezifischen Massenspeicher-Kontroller für Festplatten verwendet (wie SCSI, RAID oder Fiber Channel-Adapter).

Weitere Informationen finden Sie bei Universal Restore.

Die Treiber werden im sichtbaren Treiber-Ordner auf dem bootfähigen Medium hinterlegt. Die Treiber werden nicht in den RAM der Ziel-Maschine geladen, daher muss das Medium während der Universal Restore-Aktion eingelegt bzw. verbunden bleiben.

Das Hinzufügen von Treibern zu bootfähigen Medien ist unter folgenden Bedingungen möglich:

1. Das Acronis Backup & Recovery 11.5 Universal Restore Add-on ist auf der für die Erstellung der bootfähigen Medien verwendeten Maschine installiert UND
2. Sie erzeugen ein Wechselmedium (oder sein ISO-Abbild) oder anschließbares Medium wie einen USB-Stick. Treiber können nicht auf einen PXE Server oder WDS/RIS hochgeladen werden.

Die Treiber können zur Liste nur in Gruppen hinzugefügt werden, indem die INF-Dateien oder Ordner hinzugefügt werden, die solche Dateien enthalten. Die Wahl einzelner Treiber aus den INF-Dateien ist nicht möglich, der Media Builder informiert Sie jedoch über den Inhalt der Dateien.

So fügen Sie Treiber hinzu:

1. Klicken Sie auf **Hinzufügen** und wählen Sie dann die INF-Datei oder den die INF-Dateien enthaltenden Ordner.
2. Wählen Sie die INF-Datei oder den Ordner aus.
3. Klicken Sie auf **OK**.

Die Treiber können aus der Liste nur in Gruppen, durch Löschen der INF-Dateien, entfernt werden.

So entfernen Sie Treiber:

1. Wählen Sie die INF-Datei aus.
2. Klicken Sie auf **Entfernen**.

9.1.2 WinPE-basierte bootfähige Medien

Der Bootable Media Builder ermöglicht drei Methoden, um Acronis Backup & Recovery 11.5 in WinPE einzubinden:

- Das Acronis-Plug-in einem existierenden PE-ISO-Abbild hinzufügen. Das ist praktisch, wenn Sie das Plug-in einem früher konfigurierten, in Verwendung befindlichen PE-ISO-Abbild hinzufügen müssen.
- Ein PE-ISO-Abbild mit dem Plug-in neu erstellen.
- Das Acronis-Plug-in einer WIM-Datei zur zukünftigen Verwendung hinzufügen (manuelle ISO-Erstellung, andere Tools dem Image hinzufügen, usw.).

Der Bootable Media Builder unterstützt WinPE-Distributionen, die auf folgenden Kerneln beruhen:

- Windows Vista (PE 2.0)
- Windows Vista SP1 und Windows Server 2008 (PE 2.1).
- Windows 7 (PE 3.0), mit oder ohne das 'Supplement for Windows 7 SP1' (PE 3.1)
- Windows 8 (PE 4.0)
- Windows 8.1 (PE 5.0)

Bootable Media Builder unterstützt sowohl 32-Bit- wie auch 64-Bit-WinPE-Distributionen. Die 32-Bit-WinPE-Distributionen funktionieren auch auf 64-Bit-Hardware. Sie benötigen jedoch 64-Distributionen, um von einer Maschine booten zu können, die UEFI (Unified Extensible Firmware Interface) verwendet.

Auf WinPE 4 (und höher) basierende PE-Images benötigen ungefähr 1 GB an RAM, um arbeiten zu können.

9.1.2.1 Vorbereitung: WinPE 2.x und 3.x

Um PE 2.x oder 3.x-Images erstellen oder modifizieren zu können, installieren Sie den Bootable Media Builder auf einer Maschine, auf der das Windows Automated Installation Kit (WAIK) installiert ist. Wenn Sie keine Maschine mit AIK haben, gehen Sie wie nachfolgend beschrieben vor.

So bereiten Sie eine Maschine mit AIK vor

1. Download und Installation des Windows Automated Installation Kit.

   Automated Installation Kit (AIK) für Windows Vista (PE 2.0):

   http://www.microsoft.com/Downloads/details.aspx?displaylang=de&FamilyID=c7d4bc6d-15f3-4284-9123-679830d629f2

   Automated Installation Kit (AIK) für Windows Vista SP1 und Windows Server 2008 (PE 2.1):

   http://www.microsoft.com/Downloads/details.aspx?familyid=94BB6E34-D890-4932-81A5-5B50C657DE08&displaylang=de

   Automated Installation Kit (AIK) für Windows 7 (PE 3.0):

   http://www.microsoft.com/downloads/de-de/details.aspx?FamilyID=696DD665-9F76-4177-A811-39C26D3B3B34

   Automated Installation Kit (AIK) Supplement for Windows 7 SP1 (PE 3.1):

   http://www.microsoft.com/de-de/download/details.aspx?id=5188

   Sie können die Systemanforderungen zur Installation finden, indem Sie den unteren Links folgen.
2. [Optional] Brennen Sie das WAIK auf DVD oder kopieren Sie es auf ein Flash-Laufwerk (USB-Stick).
3. Installieren Sie Microsoft .NET Framework von diesem Kit (NETFXx86 oder NETFXx64, abhängig von Ihrer Hardware).
4. Installieren Sie Microsoft Core XML (MSXML) 5.0 oder 6.0 Parser von diesem Kit.
5. Installieren Sie Windows AIK von diesem Kit.
6. Installieren Sie Bootable Media Builder auf der gleichen Maschine.

Es ist empfehlenswert, dass Sie sich mit der dem Windows AIK beiliegenden Hilfe-Dokumentation vertraut machen. Um auf die Dokumentation zuzugreifen, wählen Sie **Microsoft Windows AIK -> Dokumentation** im Startmenü.

9.1.2.2 Vorbereitung: WinPE 4.0 und WinPE 5.0

Um Images von PE 4 oder PE 5 erstellen oder ändern zu können, installieren Sie den Bootable Media Builder auf einer Maschine, auf der das Windows Assessment and Deployment Kit (ADK) installiert ist. Wenn Sie keine Maschine mit ADK haben, gehen Sie wie nachfolgend beschrieben vor.

So bereiten Sie eine Maschine mit ADK vor

1. Laden Sie das Setup-Programm des of Assessment and Deployment Kits herunter.

   Assessment and Deployment Kit (ADK) für Windows 8 (PE 4.0): http://www.microsoft.com/de-de/download/details.aspx?id=30652.

   Assessment and Deployment Kit (ADK) für Windows 8.1 (PE 5.0): http://www.microsoft.com/de-DE/download/details.aspx?id=39982.

   Sie können die Systemanforderungen zur Installation finden, indem Sie den unteren Links folgen.
2. Installieren Sie das Assessment and Deployment Kit auf der Maschine.
3. Installieren Sie Bootable Media Builder auf der gleichen Maschine.

9.1.2.3 Das Acronis Plug-in einem WinPE-Image hinzufügen

So fügen Sie das Acronis-Plug-in einem WinPE-ISO-Abbild hinzu:

1. Wenn Sie das Plug-in der existierenden WinPE-ISO-Datei hinzufügen, entpacken Sie alle Dateien Ihrer WinPE-ISO in einen separaten Laufwerksordner.
2. Starten Sie den Bootable Media Builder entweder über die Management Konsole durch **Extras –> Bootfähiges Medium erstellen** oder als eigenständige Komponente.
3. Sollte der Agent für Windows auf der Maschine *nicht installiert* sein, dann spezifizieren einen Lizenzschlüssel oder einen License Server mit seinen Lizenzen. Die Lizenzen werden nicht zugewiesen oder neu zugewiesen. Sie helfen zu bestimmen, welche Funktionen für das erstellte Medium aktiviert werden sollen. Ohne Lizenz können Sie ein Medium erstellen, mit dem Sie nur Wiederherstellungen vom Online Backup Storage durchführen können.

   Sollte der Agent für Windows auf der Maschine *doch installiert* sein, dann übernimmt das Medium dessen Funktionalität, einschließlich Universal Restore und Deduplizierung.
4. Wählen Sie den **Typ des bootfähigen Mediums: Windows PE**.

   Wenn Sie eine neue PE-ISO-Datei erstellen:

   - Wählen Sie den Befehl **WinPE automatisch erstellen**.
   - [Optional] Aktivieren Sie zur Erstellung eines 64-Bit-Boot-Mediums das Kontrollkästchen **x64-Medium erstellen** (sofern verfügbar). Sie benötigen ein 64-Bit-Medium, um eine Maschine booten zu können, die UEFI (Unified Extensible Firmware Interface) verwendet.
   - Die Software führt das passende Skript aus und wechselt zum nächsten Fenster.

   So fügen Sie das Plug-in einem existierenden PE-ISO-Abbild hinzu:

   - Wählen Sie **WinPE-Dateien im von mir spezifizierten Ordner verwenden**.
   - Geben Sie den Pfad zum Ordner mit den WinPE-Dateien an.
5. [Optional] Wählen Sie, ob Remote-Verbindungen für eine per Boot-Medium gestartete Maschine (de)aktiviert werden sollen. Sind diese aktiviert, dann spezifizieren Sie den Benutzernamen und das Kennwort, welche auf Seiten der Konsole bei der Verbindung zum Agenten eingegeben werden sollen. Falls Sie diese Boxen leerlassen, wird die Verbindung deaktiviert.
6. Spezifizieren Sie die Netzwerkeinstellungen (S. 288) für den Netzwerkadapter der Maschine oder wählen Sie eine Autokonfiguration per DHCP.
7. [Optional] Spezifizieren Sie die Windows-Treiber, die Windows PE hinzugefügt werden sollen.

   Wenn Sie eine Maschine mit Windows PE booten, ermöglichen Ihnen diese Treiber, auf Geräte zuzugreifen, auf denen sich Ihre Backup-Archive befinden. Verwenden Sie 32-Bit-Treiber, sofern Sie eine 32-Bit-WinPE-Distribution verwenden – oder 64-Bit-Treiber, sofern Sie eine 64-Bit-WinPE-Distribution einsetzen.

   Sie können auf die hinzugefügten Treiber auch verweisen, wenn Sie Universal Restore konfigurieren. Fügen Sie zur Verwendung von Universal Restore entweder 32-Bit- oder 64-Bit-Treiber hinzu; abhängig davon, ob Sie ein 32-Bit- oder 64-Bit-Betriebssystemvariante von Windows wiederherstellen wollen.

   So fügen Sie Treiber hinzu:

   - Klicken Sie auf **Hinzufügen** und geben Sie den Pfad zur notwendigen *. inf-Datei für einen entsprechenden SCSI-, RAID- oder SATA-Controller, einen Netzwerkadapter, ein Bandlaufwerk oder andere Geräte an.
   - Wiederholen Sie dieses Prozedur für jeden Treiber, den Sie in das resultierende WinPE-Boot-Medium aufnehmen wollen.
8. Wählen Sie, ob Sie ein ISO- oder WIM-Image erstellen wollen oder das Medium auf einen Server (Acronis PXE Server, WDS oder RIS) hochgeladen werden soll.

9. Geben Sie den vollen Pfad einschließlich Dateiname zur resultierenden Image-Datei an – oder spezifizieren Sie den Server inklusive Benutzername und Kennwort für den Zugriff.
10. Überprüfen Sie Ihre Einstellungen im Fenster 'Zusammenfassung' und klicken Sie auf **Fertig stellen**.
11. Brennen Sie die ISO-Datei auf CD oder DVD (durch das Brennprogramm eines Drittherstellers) oder kopieren Sie die Daten auf ein Flash-Laufwerk wie einen USB-Stick (Daten und Flash-Laufwerk müssen zum Booten separat angepasst werden).

Sobald eine Maschine mit WinPE gebootet wird, startet Acronis Backup & Recovery 11.5 automatisch.

So erstellen Sie ein PE-Abbild (ISO-Datei) von einer resultierenden WIM-Datei:

- Ersetzen Sie die vorgegebene boot.wim-Datei im Windows PE-Ordner mit der neu erstellten WIM-Datei. Für das genannte Beispiel geben Sie ein:

  ```
  copy c:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
  ```

- verwenden Sie das Tool **Oscdimg**. Für das genannte Beispiel geben Sie ein:

  ```
  oscdimg -n –bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO
  c:\winpe_x86\winpe_x86.iso
  ```

Weitere Informationen zur Anpassung von Windows PE finden Sie im Windows PE-Benutzerhandbuch (Winpe.chm).

9.2 Verbinde mit einer Maschine, die von einem Medium gebootet wurde

Sobald eine Maschine von einem bootfähigen Medium gestartet ist, erscheint ein Konsolenfenster mit den IP-Adressen, die per DHCP oder als manuell vorkonfigurierte Werte zugewiesen wurden.

Netzwerkeinstellungen konfigurieren

Klicken Sie zum Ändern der Netzwerkeinstellungen für eine aktuelle Sitzung im Startfenster auf **Netzwerk konfigurieren**. Das erscheinende Fenster **Netzwerkeinstellungen** ermöglicht Ihnen, die Netzwerkeinstellungen für jede Netzwerkkarte (NIC) auf der Maschine zu konfigurieren.

Während einer Sitzung durchgeführte Änderungen gehen nach dem Neustart der Maschine verloren.

VLANs hinzufügen

Sie können im Fenster **Netzwerkeinstellungen** VLANs (Virtual Local Area Networks, virtuelle lokale Netzwerke) hinzufügen. Verwenden Sie diese Funktionalität, falls Sie auf einen Backup-Speicherort zugreifen müssen, der sich in einem spezifischen VLAN befindet.

VLANs werden hauptsächlich dazu verwendet, um lokale Netzwerke (LANs) in logische Teilnetze zu segmentieren. Eine Netzwerkkarte (NIC), die mit einem *Zugriffs*-Port des Switches verbunden ist, kann immer auf das in der Port-Konfiguration spezifizierte VLAN zugreifen. Eine Netzwerkkarte (NIC), die mit einem *Trunk*-Port des Switches verbunden ist, kann nur dann auf die in der Port-Konfiguration erlaubten VLANs zugreifen, wenn Sie die VLANs in den Netzwerkeinstellungen spezifizieren.

So ermöglichen Sie den Zugriff auf ein VLAN über einen Trunk-Port

1. Klicken Sie auf **VLAN hinzufügen**.
2. Wählen Sie die Netzwerkkarte aus, die Zugriff auf dasjenige lokale Netzwerk bereitstellt, welches das benötigte VLAN enthält.
3. Spezifizieren Sie den VLAN-Bezeichner (Identifier).

Nachdem Sie auf **OK** geklickt haben, erscheint in der Liste der Netzwerkadapter ein neuer Eintrag.

Sollten Sie ein VLAN entfernen wollen, dann klicken Sie auf den erforderlichen VLAN-Eintrag – und anschließend auf **VLAN entfernen**.

Lokale Verbindung

Um direkt auf einer Maschine arbeiten zu können, die mit einem bootfähigen Medium gestartet wurde, müssen Sie im Startfenster auf **Diese Maschine lokal verwalten** klicken.

Remote-Verbindung

Um eine Management Konsole mit einer Remote-Maschine zu verbinden, die mit einem bootfähigen Medium gestartet wurde, müssen Sie im Konsolen-Menü die Befehle **Verbinden –> Remote-Maschine verwalten** wählen. Spezifizieren Sie anschließend eine der IP-Adressen der Maschine. Geben Sie Anmeldedaten (Benutzername, Kennwort) ein, falls diese bei Erstellung des Bootmediums konfiguriert wurden.

9.3 Mit bootfähigen Medien arbeiten

Die Arbeitsweise mit einer Maschine, die per bootfähigem Medium gestartet wurde, ist sehr ähnlich zu den Backup- und Recovery-Aktionen unter dem sonst üblichen Betriebssystem. Der Unterschied ist folgender:

1. Unter einem Windows-typischen bootfähigen Medium hat ein Volume denselben Laufwerksbuchstaben wie unter Windows. Volumes, die unter Windows keine Laufwerksbuchstaben haben (wie etwa das Volume **System-reserviert**) bekommen freie Laufwerksbuchstaben in der Reihenfolge ihres Vorkommens auf den Laufwerken zugewiesen.

   Sollte das bootfähige Medium kein Windows auf der Maschine erkennen können oder mehrere Windows-Versionen erkennen, dann wird allen Volumes (einschließlich derer ohne Laufwerksbuchstaben) in der Reihenfolge ihres Vorkommens auf den Laufwerken ein Buchstabe zugewiesen. Auf diese Art können die Laufwerksbuchstaben dann von denen unter Windows vorliegenden abweichen. So könnte beispielsweise die Zuordnung des Laufwerks D: unter dem bootfähigen Medium dem Laufwerk E: entsprechen, welches Windows verwendet.

   Achtung! Um auf der sicheren Seite zu sein, ist es ratsam, den jeweils verwendeten Volumes eindeutige Namen zuzuweisen.

2. Ein Linux-typisches bootfähiges Medium zeigt lokale Laufwerke und Volumes als 'unmounted' an (sda1, sda2...).
3. Mit einem bootfähigen Medium erstellte Backups werden mit einer vereinfachten Dateibenennung (S. 83) gekennzeichnet. Backups erhalten nur dann Standardnamen, wenn diese einem bereits existierenden Archiv, welches einen Standarddateinamen verwendet, hinzugefügt werden – oder falls der Zielort keine vereinfachte Dateibenennung unterstützt.
4. Ein bootfähiges Medium im Stil 'Linux-typisch' kann keine Backups auf ein NTFS-formatiertes Volume schreiben. Wechseln Sie zum Stil 'Windows-typisch', wenn Sie diese Funktion benötigen.
5. Sie können den Arbeitsstil des bootfähigen Mediums zwischen Windows- und Linux-typisch umschalten, indem Sie **Extras** –> **Volume-Darstellung ändern** wählen.
6. Der Verzeichnisbaum **Navigation** ist in der Benutzeroberfläche des Mediums nicht vorhanden. Verwenden Sie den Menübefehl **Navigation**, um zwischen verschiedenen Ansichten umzuschalten.
7. Es können keine geplanten Tasks benutzt werden, da grundsätzlich keine Tasks erstellt werden können. Um eine Aktion zu wiederholen, konfigurieren Sie sie von Anfang an neu.

8. Der Speicherzeitraum für Ereignisse (Logs) ist auf die aktuelle Sitzung beschränkt. Sie können die gesamte Ereignisliste oder gefilterte Logs in eine Datei speichern.
9. Zentrale Depots werden im Verzeichnisbaum des Fensters **Archiv** nicht angezeigt.

   Um auf ein verwaltetes Depot zuzugreifen, geben Sie im Feld **Pfad** ein:

   bsp://knoten_adresse/depot_name/

   Um auf ein zentrales, nicht verwaltetes Depot zuzugreifen, tragen Sie den vollen Pfad zum Ordner des Depots ein.

   Nach Eingabe der Anmeldedaten sehen Sie eine Liste der Archive, die sich im Depot befinden.

9.3.1 Einen Anzeigemodus einstellen

Bei einer von einem bootfähigen Medium gestarten Maschine wird der Anzeigemodus basierend auf der Hardware-Konfiguration automatisch erkannt (Monitor- und Grafikkarten-Spezifikationen). Sollte aus irgendeinem Grund der Darstellungsmodus nicht korrekt erkannt werden, gehen Sie folgendermaßen vor:

1. Drücken Sie im Boot-Menü auf F11.
2. Geben Sie in die Eingabeaufforderung folgenden Befehl ein: **vga=ask**, fahren Sie dann mit dem Boot-Vorgang fort.
3. Wählen Sie aus der Liste der verfügbaren Darstellungsmodi den passenden durch Eingabe seiner Nummer (z.B. **318**), drücken Sie dann auf Enter.

Falls Sie diese Schritte nicht jedes Mal ausführen möchten, wenn Sie auf einer bestimmten Hardwarekonfiguration von einem Boot-Medium starten, erstellen Sie das Medium mit der entsprechenden Modus-Nummer (in unserem Beispiel: **vga=0x318**) im Fenster **Kernel-Parameter** (weitere Informationen finden Sie im Abschnitt Bootable Media Builder (S. 285)).

9.3.2 iSCSI- und NDAS-Geräte konfigurieren

Dieser Abschnitt beschreibt, wie iSCSI (Internet Small Computer System Interface)- und NDAS (Network Direct Attached Storage)-Geräte bei der Arbeit mit bootfähigen Medien konfiguriert werden.

Diese Geräte sind über eine Netzwerkschnittstelle mit der Maschine verbunden und werden angezeigt, als wären sie lokal angeschlossene Geräte. Im Netzwerk werden iSCSI-Geräte über ihre IP-Adresse und NDAS-Geräte über ihre Geräte-ID identifiziert.

iSCSI-Geräte werden manchmal auch als iSCSI-Target bezeichnet. Eine Hard- oder Software-Komponente, die das Zusammenspiel von Maschine und iSCSI-Target ermöglicht, wird als iSCSI-Initiator bezeichnet. Der Name des iSCSI-Initiators wird üblicherweise durch den Administrator des Servers bestimmt, der das Gerät hostet.

So fügen Sie ein iSCSI-Gerät hinzu

1. Führen sie in einem (Linux- oder PE-basierten) Boot-Medium die Management Konsole aus.
2. Klicken Sie auf **iSCSI/NDAS-Geräte konfigurieren** (in einem Linux-basierten Medium) bzw. auf **iSCSI-Setup ausführen** (in einem PE-basierten Medium).
3. Geben Sie vom Host des iSCSI-Gerät die IP-Adresse und den Port an und zudem den Namen des iSCSI-Initiators.
4. Benötigt der Host eine Authentifizierung, dann geben Sie Benutzernamen und Kennwort ein.
5. Klicken Sie auf **OK**.
6. Wählen Sie das iSCSI-Gerät aus der Liste und klicken Sie dann auf **Verbinden**.

7. Spezifizieren Sie bei Erscheinen einer Eingabeaufforderung Benutzernamen und Kennwort, um auf das iSCSI-Gerät zugreifen zu können.

So fügen Sie ein NDAS-Gerät hinzu

1. Führen sie in einem Linux-basierten Boot-Medium die Management Konsole aus.
2. Klicken Sie auf **iSCSI/NDAS-Geräte konfigurieren**.
3. Klicken Sie in **NDAS-Geräte** auf **Gerät hinzufügen**.
4. Geben Sie die 20-stellige Geräte-ID an.
5. Geben Sie den fünfstelligen Schreibschlüssel an, wenn Sie erlauben wollen, dass Daten auf das Gerät geschrieben werden. Ohne diesen Schlüssel wird das Gerät nur im 'Read-only'-Modus verfügbar sein.
6. Klicken Sie auf **OK**.

9.4 Liste verfügbarer Befehle und Werkzeuge in Linux-basierten bootfähigen Medien

Linux-basierte Boot-Medien enthalten folgende Kommandos und Befehlszeilen-Werkzeuge, die Sie bei Ausführung einer Eingabeaufforderung nutzen können. Zum Starten der Eingabeaufforderung drücken Sie Strg+Alt+F2, während Sie in der Management Konsole des bootfähigen Mediums sind.

Acronis Command-Line Utilities

- `acrocmd`
- `acronis`
- `asamba`
- `lash`

Linux-Befehle und Werkzeuge

busybox	ifconfig	rm
cat	init	rmmod
cdrecord	insmod	route
chmod	iscsiadm	scp
chown	kill	scsi_id
chroot	kpartx	sed
cp	ln	sg_map26
dd	ls	sh
df	lspci	sleep
dmesg	lvm	ssh
dmraid	mdadm	sshd
e2fsck	mkdir	strace
e2label	mke2fs	swapoff
echo	mknod	swapon

```
egrep      mkswap      sysinfo
fdisk      more        tar
fsck       mount       tune2fs
fxload     mtx         udev
gawk       mv          udevinfo
gpm        pccardctl   udevstart
grep       ping        umount
growisofs  pktsetup    uuidgen
grub       poweroff    vconfig
gunzip     ps          vi
halt       raidautorun zcat
hexdump    readcd
hotplug    reboot
```

9.5 Acronis Startup Recovery Manager

Der Acronis Startup Recovery Manager ist eine Modifikation des bootfдhigen Agenten (S. 487), befindet sich unter Windows auf der Systemfestplatte bzw. unter Linux auf der /boot-Partition und ist so konfiguriert, dass er durch Drücken von F11 während des Boot-Vorgangs gestartet wird. Dies bietet eine Alternative zum Start des bootfähigen Notfallwerkzeugs über ein separates Medium oder eine Netzwerkverbindung.

Der Acronis Startup Recovery Manager ist besonders für mobile Anwender nützlich. Wenn ein Fehler auftritt, booten Sie die Maschine neu und drücken die F11-Taste, sobald die Meldung „Druecken Sie F11 zum Ausfuehren des Acronis Startup Recovery Managers…" erscheint. Darauf wird das Programm gestartet und Sie können die Wiederherstellung durchführen.

Sie können außerdem auch Backups mit dem Acronis Startup Recovery Manager erstellen, wenn sie unterwegs sind.

Auf Maschinen, die einen GRUB Boot-Loader installiert haben, wählen Sie den Acronis Startup Recovery Manager aus dem Boot-Menü, statt F11 zu drücken.

Aktivieren

Die Aktivierung schaltet die Boot-Meldung „Druecken Sie F11 zum Ausfuehren des Acronis Startup Recovery Manager…" ein (sofern Sie keinen GRUB Boot-Loader haben) oder fügt den Menü-Eintrag „Acronis Startup Recovery Manager" zum Menü von GRUB hinzu (sofern Sie GRUB haben).

Auf der Systemfestplatte (bzw. der /boot-Partition unter Linux) sollten mindestens 100 MB freier Speicherplatz verfügbar sein, um den Acronis Startup Recovery Manager zu aktivieren.

Die Aktivierung des Acronis Startup Recovery Manager überschreibt den Master Boot Record (MBR) mit seinem eigenen Boot-Code, außer Sie verwenden den GRUB Boot-Loader und dieser ist im MBR installiert. Daher müssen Sie möglicherweise auch die Boot-Loader von Drittherstellern reaktivieren, wenn diese installiert sind.

Wenn Sie unter Linux einen anderen Boot-Loader als GRUB verwenden (etwa LILO), sollten Sie erwägen, diesen statt in den MBR in den Boot-Record einer Linux-root- oder Boot-Partition zu installieren, bevor Sie den Acronis Startup Recovery Manager aktivieren. Konfigurieren Sie anderenfalls den Boot-Loader manuell nach der Aktivierung.

Nicht aktivieren

Deaktiviert die Boot-Meldung „Druecken Sie F11 zum Ausfuehren des Acronis Startup Recovery Managers...“ (oder den Menü-Eintrag in GRUB). Falls der Acronis Startup Recovery Manager nicht aktiviert ist, müssen Sie zur Wiederherstellung eines nicht mehr bootfähigen Systems Folgendes tun:

- Booten Sie die Maschine mit Hilfe eines separaten, bootfähigen Notfallmediums.
- Verwenden Sie einen Netzwerk-Boot von einem Acronis PXE Server oder Microsoft Remote Installation Services (RIS).

9.6 Acronis PXE Server

Der Acronis PXE Server ermöglicht es, Maschinen mit den 'Acronis Bootfähigen Komponenten' über das Netzwerk zu starten.

Netzwerk-Booten:

- eliminiert die Notwendigkeit eines Technikers vor Ort, um das bootfähige Medium in das zu bootende System einzulegen
- reduziert bei Gruppen-Operationen die zum Booten mehrerer Maschinen benötigte Zeit (im Vergleich zu physikalischen Bootmedien).

Bootfähige Komponenten werden vom Acronis Bootable Media Builder zum Acronis PXE Server hochgeladen. Um eine bootfähige Komponente hochzuladen, starten Sie den Bootable Media Builder (entweder über die Management Konsole durch **Extras –> Bootfähiges Medium erstellen** oder als eigene Komponente) und folgen Sie dann den Schritt-für-Schritt-Anweisungen, die detailliert im Abschnitt „Bootable Media Builder (S. 285)“ beschrieben sind.

Das Booten mehrerer Maschinen über den Acronis PXE Server macht insbesondere Sinn, wenn im Netzwerk ein Dynamic Host Control Protocol (DHCP)-Server vorhanden ist. Dann erhalten die Netzwerkadapter der gebooteten Maschinen automatisch eine IP-Adresse.

Einschränkung:

Der Acronis PXE Server unterstützt keine UEFI-Boot-Loader.

9.6.1 Acronis PXE Server-Installation

Den Acronis PXE Server installieren

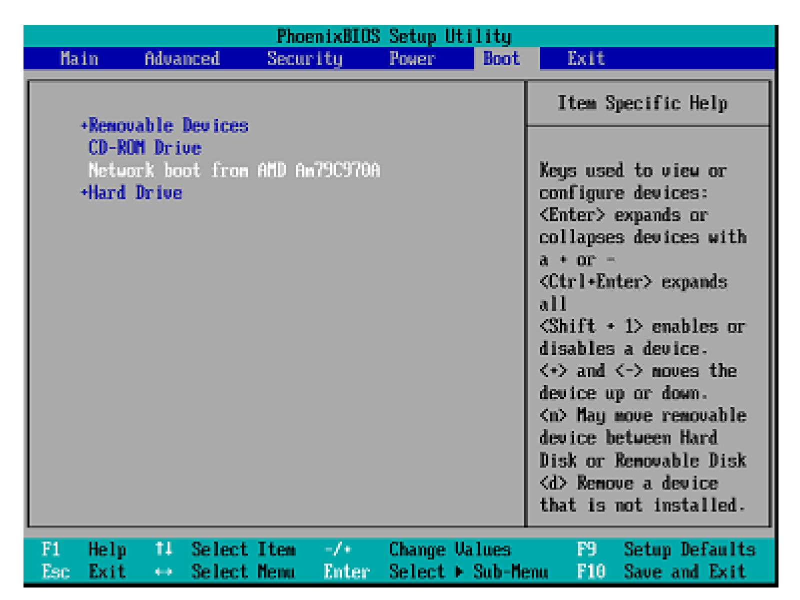
1. Führen Sie die Setup-Datei von Acronis Backup & Recovery 11.5 aus.
2. Wählen Sie den Acronis PXE Server von der Liste der **Komponenten für zentrale Verwaltung**.
3. Folgen Sie den Bildschirmanweisungen.

Acronis PXE Server läuft unmittelbar nach der Installation als Dienst. Später wird er automatisch nach jedem System-Neustart ausgeführt. Sie können den Acronis PXE Server so wie jeden anderen Windows-Dienst starten oder stoppen.

9.6.2 Eine Maschine für das Booten von PXE konfigurieren

Für fabrikneue Maschinen reicht es aus, dass ihr BIOS das Booten von Netzwerk unterstützt.

Auf einer Maschine, die ein Betriebssystem auf ihrer Festplatte hat, muss das BIOS so konfiguriert werden, dass der Netzwerkadapter entweder das erste Boot-Gerät ist – oder zumindest vor der Festplatte aufgelistet ist. Das Beispiel zeigt eine typische BIOS-Konfiguration. Wenn Sie kein bootfähiges Medium einlegen, wird die Maschine vom Netz booten.



In einigen BIOS-Versionen müssen Sie die geänderten BIOS-Einstellungen, nach Aktivierung des Netzwerkadapters, erst abspeichern, damit die Netzwerkkarte in der Liste der Boot-Geräte erscheint.

Sollte Ihre Hardware mehrere Netzwerkadapter haben, so stellen Sie sicher, dass das Netzwerkkabel auch in der vom BIOS unterstützten Karte steckt.

9.6.3 Über Subnetze hinweg arbeiten

Damit der Acronis PXE Server auch in anderen Subnetzen arbeiten kann (über einen Switch hinweg), muss der Switch PXE-Netzwerkverkehr weiterreichen können. Die IP-Adressen des PXE Servers sind auf Pro-Netzwerkadapter-Basis konfiguriert, unter Verwendung von IP-Helfer-Funktionalität wie bei DHCP-Server-Adressen. Für mehr Informationen schlagen Sie hier nach: http://support.microsoft.com/kb/257579/de.

10 Laufwerksverwaltung

Acronis Disk Director Lite ist ein Tool, das dazu dient, die Laufwerks-/Volume-Konfiguration einer Maschine für Wiederherstellungen von Volume-Images vorzubereiten, die per Acronis Backup & Recovery 11.5-Software erstellt wurden.

Nachdem ein Laufwerk gesichert und sein Image an einem sicheren Speicherplatz hinterlegt wurde, kann es vorkommen, dass sich die Laufwerkskonfiguration der Maschine durch Austausch einer Festplatte oder durch Hardware-Verlust ändert. In diesem Fall hat der Benutzer durch die Hilfe des Acronis Disk Director Lite die Möglichkeit, die notwendige Laufwerkskonfiguration wieder so zu erstellen, dass das Laufwerksabbild exakt 'wie es war' wiederhergestellt werden kann (oder mit jeder Abweichung der Laufwerk-/Volume-Struktur, die der Benutzer für notwendig hält).

Alle Laufwerk- und Volume-Aktionen bergen ein gewisses Risiko von Datenverlust. Aktionen auf System- oder Daten-Volumes müssen sehr sorgfältig ausgeführt werden, um mögliche Probleme mit dem Boot-Ablauf oder Laufwerksdatenspeicher zu vermeiden.

Aktionen mit Laufwerken und Volumes benötigen eine gewisse Zeit – und Stromverlust, unbeabsichtigtes Ausschalten der Maschine oder versehentliches Drücken des Reset-Schalters während der Prozedur können zur Beschädigung des Volumes und Datenverlust führen.

Alle Aktionen mit den Volumes dynamischer Laufwerke in Windows XP und Windows 2000 setzen voraus, dass der Acronis Managed Machine Service unter einem Benutzerkonto mit Administrator-Rechten ausgeführt wird.

Treffen Sie alle notwendigen Vorsichtsmaßnahmen (S. 300), um einen möglichen Datenverlust zu vermeiden.

10.1 Unterstützte Dateisysteme

Der Acronis Disk Director Lite unterstützt die folgenden Dateisysteme:

- FAT 16/32
- NTFS

Wenn Sie mit einem Volume, das ein andere Dateisystem hat, eine Aktion durchzuführen müssen, dann verwenden Sie die Vollversion des Acronis Disk Director. Dieses Programm bietet noch mehr Tools und Utilities, um Festplatten und Volumes mit den folgenden Dateisystemen zu verwalten:

- FAT 16/32
- NTFS
- Ext2
- Ext3
- HFS+
- HFSX
- ReiserFS
- JFS
- Linux SWAP

10.2 Grundlegende Vorsichtsmaßnahmen

Treffen Sie alle notwendigen Vorsichtsmaßnahmen, um mögliche Schäden an der Laufwerks- bzw. Volume-Struktur oder Datenverlust abzuwenden und beachten Sie folgende grundsätzliche Regeln:

1. Erstellen Sie von Laufwerken, auf denen Volumes erstellt oder verwaltet werden, ein Backup. Indem Sie wichtige Daten auf ein anderes Laufwerk, eine Netzwerkfreigabe oder Wechselmedien sichern, können Sie – wohl wissend, dass Ihre Daten gut geschützt sind – beruhigt mit Ihren Laufwerken bzw. Volumes arbeiten.
2. Überprüfen Sie Ihre Festplatte, um sicherzustellen, dass sie voll funktionstüchtig ist und keine defekten Sektoren oder Dateisystemfehler enthält.
3. Führen Sie keine Laufwerks- bzw. Volume-Aktionen aus, während andere Programme mit Low-Level-Zugriff auf Laufwerke ausgeführt werden. Beenden Sie diese Programme bevor Sie Acronis Disk Director Lite ausführen.

Durch diese einfachen Vorsichtsmaßnahmen schützen Sie sich vor versehentlichem Datenverlust.

10.3 Acronis Disk Director Lite ausführen

Sie können Acronis Disk Director Lite unter Windows oder über ein bootfähiges Medium ausführen.

Beschränkungen

- Der Acronis Disk Director Lite ist unter bzw. für Windows 8/8.1 und für den Windows Server 2012/2012 R2 nicht verfügbar.
- Aktionen zur Laufwerksverwaltung funktionieren unter einem bootfähigen Medium möglicherweise nicht korrekt, falls auf der Maschine Speicherplätze (Storage Spaces) konfiguriert sind.

Acronis Disk Director Lite unter Windows ausführen

Wenn Sie die Acronis Backup & Recovery 11.5 Management Console starten und mit einer verwalteten Maschine verbinden, steht die Ansicht **Laufwerksverwaltung** im Zweig **Navigation** der Konsole zur Verfügung, von wo aus Sie den Acronis Disk Director Lite starten können.

Acronis Disk Director Lite von einem bootfähigen Medium ausführen

Sie können Acronis Disk Director Lite auf einer fabrikneuen, einer Nicht-Windows-Maschine oder einer, die nicht booten kann, ausführen. Um dies zu tun, booten Sie die Maschine von einem bootfдhigen Medium (S. 487), das mit dem Acronis Bootable Media Builder erstellt wurde; starten die Management Konsole und klicken dann auf **Laufwerksverwaltung**.

10.4 Auswählen des Betriebssystems für die Datenträgerverwaltung

Auf einer Maschine mit zwei oder mehr Betriebssystemen hängt die Darstellung der Datenträger und Volumes davon ab, welches Betriebssystem gerade ausgeführt wird.

Ein Volume kann in verschiedenen Windows-Betriebssystemen auch unterschiedliche Buchstaben haben. Es kann z.B. sein, dass Volume „E:“ als „D:“ oder „L:“ angezeigt wird, wenn Sie ein anderes Windows-Betriebssystem booten, das auf derselben Maschine installiert ist. (Es ist aber auch möglich, dass dieses Volume unter allen auf der Maschine installierten Windows-Betriebssystemen als „E:“ angezeigt wird.)

Ein unter einem Windows-Betriebssystem erstellter dynamischer Datenträger wird in einem anderen Betriebssystem als **Fremder Datenträger** angesehen oder möglicherweise von diesem Betriebssystem gar nicht unterstützt.

Wenn Sie eine Aktion zur Datenträgerverwaltung mit einer solchen Maschine ausführen müssen, dann müssen Sie angeben, für welches Betriebssystem das Laufwerkslayout angezeigt und die Datenträgerverwaltungsaktion ausgeführt wird.

Der Name des aktuell ausgewählten Betriebssystems wird in der Symbolleiste der Konsole hinter **Das aktuelle Laufwerkslayout ist für:** angezeigt. Um ein anderes Betriebssystem auszuwählen, klicken Sie im Fenster **Auswahl des Betriebssystems** auf den Namen des Betriebssystems. Dieses Fenster wird unter den bootfähigen Medien angezeigt, nachdem Sie auf **Laufwerksverwaltung** geklickt haben. Das Laufwerkslayout wird so angezeigt, wie es dem ausgewählten Betriebssystem entspricht.

10.5 Ansicht „Laufwerksverwaltung"

Acronis Disk Director Lite wird über die **Laufwerksverwaltung**-Ansicht der Konsole kontrolliert.

Der oberste Bereich der Ansicht enthält eine Laufwerks- und Volume-Tabelle mit der Möglichkeit zur Sortierung, zur Anpassung der Spalten und verfügt über eine Symbolleiste. Die Tabelle präsentiert alle verfügbaren Laufwerke, zugewiesene Laufwerksbuchstaben und -bezeichnungen, Laufwerkstyp sowie -kapazität, freien und benutzten Speicherplatz, Dateisystem und Status eines jeden Laufwerks. Die Symbolleiste beinhaltet Icons zum Starten der Aktionen **Rückgängig**, **Wiederherstellen**und **Ausführen**, die sich auf ausstehende Aktionen (S. 316) beziehen.

Über den grafischen Bereich im unteren Teil der Ansicht werden alle Laufwerke und ihre Volumes noch einmal als Rechtecke visualisiert, inklusive ihrer Basisdaten (Bezeichnung, Laufwerksbuchstabe, Größe, Status, Typ und Dateisystem).

Beide Teile der Ansicht bilden zudem den verfügbaren nicht zugeordneten Speicherplatz ab, der zur Erstellung von Laufwerken verwendet werden kann.

Aktionen starten

Jede Aktion kann folgendermaßen gestartet werden:

- vom Kontextmenü der Laufwerke oder Festplatten (in der Tabelle und in der grafischen Ansicht)
- aus dem Menü **Laufwerksverwaltung** der Konsole
- aus dem Bereich **Aktionen** auf der Seitenleiste **Aktionen und Werkzeuge**

*Beachten Sie, dass die Liste verfügbarer Aktionen im Kontextmenü, im Menü **Auswahl** und im Seitenleistenbereich **Aktionen** vom ausgewählten Volume- oder Laufwerkstyp abhängt. Dasselbe trifft auch für nicht zugeordneten Speicher zu.*

Ergebnisanzeige von Aktionen

Die Ergebnisse aller geplanten Festplatten- oder Laufwerksaktionen werden sofort in der Ansicht **Laufwerksverwaltung** der Konsole angezeigt. Wenn Sie z.B. ein Laufwerk erstellen, wird dies sofort angezeigt – und zwar sowohl in der Tabelle als auch in der unteren, grafischen Ansicht. Auch alle anderen Laufwerksänderungen, inklusive geänderter Laufwerksbuchstaben oder -bezeichnungen, werden sofort in der Ansicht dargestellt.

10.6 Festplattenaktionen

Acronis Disk Director Lite ermöglicht folgende auf Festplatten anwendbare Aktionen:

- Disk Initialisierung (S. 303) – richtet neue, dem System hinzuzufügende Hardware ein
- Einfaches Festplatten-Klonen (S. 304) – überträgt die kompletten Daten einer Quell- auf eine Zielplatte (Basisdatenträger vom MBR-Typ)

- Festplatten konvertieren: MBR zu GPT (S. 306) – konvertiert eine MBR-Partitionstabelle zu GPT
- Festplatten konvertieren: GPT zu MBR (S. 307) – konvertiert eine GPT-Partitionstabelle zu MBR
- Festplatten konvertieren: Basis zu Dynamisch (S. 307) – konvertiert einen Basis- zu einem dynamischen Datenträger
- Festplatten konvertieren: Dynamisch zu Basis (S. 308) – konvertiert einen dynamischen zu einem Basisdatenträger

Die Vollversion des Acronis Disk Director verfügt über weitere Werkzeuge zum Arbeiten mit Festplatten.

Acronis Disk Director Lite benötigt einen exklusiven Zugriff auf das Ziellaufwerk. Das bedeutet, dass dann auch kein anderes Disk ManagementLaufwerksverwaltung-Werkzeug (etwa die Windows Datenträgerverwaltung) auf sie zugreifen kann. Sollten Sie eine Meldung erhalten, dass das Laufwerk nicht blockiert werden kann, so schließen Sie das die Platte gerade benutzende Laufwerksverwaltung-Werkzeug und starten erneut. Schließen Sie alle aktiven Festplatten-Werkzeuge, sofern Sie nicht bestimmen können, welche Anwendung das Laufwerk gerade blockiert.

10.6.1 Festplatten-Initialisierung

Wenn Sie dem System eine neue Festplatte hinzufügen, so erkennt Acronis Disk Director Lite die veränderte Konfiguration und integriert die neue Platte in die Liste aktueller Laufwerke und Volumes. Sollte die Festplatte noch nicht initialisiert sein oder ein unbekanntes Dateisystem verwenden, so können Sie noch keine Programme auf ihr installieren und keine Daten auf ihr speichern.

In diesem Fall wird Acronis Disk Director Lite erkennen, dass die Festplatte verwendet werden kann, und die Notwendigkeit, diese zu initialisieren. Das Fenster **Laufwerksverwaltung** stellt die neu erkannte Hardware als grauen Balken mit grauem Symbol dar, um so die Nichtverwendbarkeit zu visualisieren.

So initialisieren Sie ein Laufwerk:

1. Wählen das zu initialisierende Laufwerk.
2. Klicken Sie mit der rechten Maustaste auf das gewählte Volume und wählen Sie im Kontextmenü **Initialisieren**. Das nachfolgende Fenster **Disk-Initialisierung** versorgt Sie mit grundlegenden Hardware-Details wie Laufwerksnummer oder Kapazität und bietet an, Sie bei der Wahl Ihrer nun möglichen Aktionen zu unterstützen.
3. Sie können in diesem Fenster das Partitionsschema der Disk (MBR oder GPT) und den Disk-Typ (Basis oder Dynamisch) einstellen. Die neue Laufwerksstatus wird sofort grafisch in der **Laufwerksverwaltung**-Ansicht der Konsole angezeigt.
4. Indem Sie auf **OK** klicken, fügen Sie die Disk-Initialisierung der Liste ausstehender Aktionen hinzu.

(Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausfьhren (S. 316). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

Nach der Initialisierung bleibt der ganze Festplattenplatz unzugeorndet und kann daher für die Programminstallation oder zur Dateiaufbewahrung nicht benutzt zu werden. Um den Speicherplatz verfügbar zu machen, fahren Sie nun normalerweise mit der Aktion **Volume erstellen** fort.

Wenn Sie weitere Einstellungen des Laufwerks ändern wollen, so können Sie dafür auch später noch die Werkzeuge von Acronis Disk Director Lite verwenden.

10.6.2 Einfaches Festplatten-Klonen

Manchmal ist es notwendig, alle Daten einer Festplatte auf eine andere zu übertragen. Typische Gründe sind eine Vergrößerung des Systemlaufwerks, die Einrichtung eines neuen Systems oder die Räumung des Laufwerks aufgrund eines Hardware-Fehlers. Wie auch immer: die Gründe für die Aktion **Basisdatenträger klonen** können als Notwendigkeit zum exakten Transfer aller Daten einer Quell- auf eine Zielplatte zusammengefasst werden.

Acronis Disk Director Lite ermöglicht Ihnen die Durchführung der Aktion nur mit Basisdatenträgern mit MBR-Partitionsschema.

So planen Sie die Aktion **Basisdatenträger klonen**:

1. Wählen Sie die zu klonende Festplatte.
2. Bestimmen Sie die Zielfestplatte für die Klonaktion.
3. Wählen Sie die Methoden zum Klonen und spezifizieren Sie zusätzliche Optionen.

Die neue Laufwerksstruktur wird sofort in der **Laufwerksverwaltung**-Ansicht angezeigt.

*Es wird empfohlen, einen aktivierten Acronis Startup Recovery Manager (S. 484) (ASRM) zu deaktivieren, bevor Sie ein Systemlaufwerk klonen. Andernfalls könnte das geklonte Betriebssystem möglicherweise nicht starten. Nach dem Klonen können Sie den ASRM aktivieren. Wenn die Deaktivierung nicht möglich ist, dann wählen Sie die Methode **Wie vorliegend**, um die Festplatte zu klonen.*

10.6.2.1 Quell- und Zielfestplatten bestimmen

Das Programm zeigt eine Liste aller partitionierten Laufwerke und fordert den Anwender dann auf, die Quelle zu wählen, von der die Daten zu einer anderen Platte übertragen werden.

Als Nächstes folgt die Wahl der Zielfestplatte für die Klonaktion. Das Programm ermöglicht die Wahl nur solcher Laufwerke, deren Größe ausreichend ist, um alle Daten des Quelllaufwerks verlustfrei aufzunehmen.

Sollten sich auf der gewählten Zielfestplatte Daten befinden, wird eine Warnung angezeigt: "**Das gewählte Ziellaufwerk ist nicht leer. Die Daten auf dem Laufwerk werden überschrieben.**", was bedeutet, dass alle derzeit auf dem gewählten Laufwerk verfügbaren Daten unwiederbringlich verloren gehen.

10.6.2.2 Klon-Methoden und erweiterte Optionen

Die Aktion **Basis-Laufwerk klonen** bedeutet normalerweise, dass alle Informationen des Quelllaufwerks "**Wie vorliegend**" auf das Ziellaufwerk übertragen werden. Sollte also das Zielllaufwerk gleich groß oder größer sein, so können alle Informationen exakt wie auf der Quelle gespeichert übertragen werden.

Durch die große Bandbreite verfügbarer Hardware ist es jedoch durchaus normal, dass das Ziellaufwerk eine andere Größe als die Quelle hat. Sollte das Ziellaufwerk größer sein, so kann es ratsam sein, unter Verwendung der Option **Volumes proportional anpassen** die Quelllaufwerke so anzupassen, dass auf dem Ziel nicht zugeordneter Speicherplatz vermieden wird. Die Option **Basisdatenträger klonen** „wie vorliegend" bleibt bestehen, nur wird die Standardmethode zum Klonen inkl. proportionaler Vergrößerung aller **Quell-**-Laufwerke so durchgeführt, dass auf der **Ziel**-Festplatte kein nicht zugeordneter Speicherplatz verbleibt.

Ist das Ziel kleiner, so steht die Option **Wie vorliegend** nicht mehr zur Verfügung wird die proportionale Größenanpassung **Quell**-Laufwerke zwingend notwendig. Das Programm analysiert das

Ziellaufwerk daraufhin, ob seine Größe ausreicht, alle Daten des **Quelllaufwerks** verlustfrei aufnehmen zu können. Nur wenn ein Transfer mit proportionaler Größenanpassung der **Quell**-Laufwerke ohne Datenverlust möglich ist, kann der Anwender mit der Aktion fortfahren. Sollte wegen einer Größenbeschränkung eine sichere Übertragung der **Quell**-Daten auf das **Ziel**-Laufwerk auch mit proportionaler Größenanpassung nicht möglich sein, dann die Aktion **Basis-Laufwerk klonen** nicht mehr fortgesetzt werden.

Wenn Sie vorhaben, ein Laufwerk zu klonen, das ein **System-Volume** enthält, sollten Sie die **Erweiterten Optionen** beachten.

Indem Sie auf **Abschluss** klicken, fügen Sie das Laufwerk-Klonen der Liste ausstehender Aktionen hinzu.

(Damit die hinzugefügte Aktion durchgeführt werden, müssen Sie diese ausfьhren (S. 316) lassen. Wenn Sie das Programm ohne Ausführung der offenen Aktionen beenden, werden diese alle verworfen.)

Erweiterte Optionen verwenden

Wenn Sie ein Laufwerk klonen, das ein **System-Volume** enthält, müssen Sie auch die Bootfähigkeit des Betriebssystems für das Ziellaufwerk bewahren. Das bedeutet, dass das Betriebssystem System-Laufwerks-Informationen (z.B. Laufwerksbuchstabe) erhalten muss, die zur NT-Festplatten-Signatur passen (welche im Master Boot Record hinterlegt ist). Zwei Festplatten mit derselben NT-Signatur können jedoch nicht richtig unter einem Betriebssystem arbeiten.

Wenn aber auf einer Maschine zwei Festplatten, die ein System-Laufwerk enthalten, dieselbe NT-Signatur haben, so startet das Betriebssystem von der ersten Festplatte, erkennt dabei die gleiche Signatur auf der zweiten Festplatte, erzeugt automatisch eine neue, eindeutige NT-Signatur und weist diese dann der zweiten Platte zu. Als Konsequenz verlieren darauf dann alle Volumes des zweiten Laufwerks ihre Laufwerksbuchstaben, werden Verzeichnispfade ungültig und können Programme ihre Dateien nicht mehr finden. Das Betriebssystem auf diesem Laufwerk kann daher auch nicht mehr booten.

Ihnen stehen zwei Alternativen zur Verfügung, um die Bootfähigkeit auf dem Ziellaufwerk zu erhalten:

1. Kopieren der NT-Signatur – um die Zielfestplatte mit der NT-Signatur zu versehen, die zu den ebenfalls auf die Platte kopierten Registry-Schlüsseln passt
2. NT-Signatur belassen – um die alte Disk-Signatur des Ziellaufwerks zu bewahren und das Betriebssystem an diese anzupassen

Falls Sie die NT-Signatur kopieren müssen:

1. Aktivieren Sie das Kontrollkästchen **NT-Signatur kopieren**. Sie erhalten eine Warnung: "Wenn sich auf der Festplatte ein Betriebssystem befindet, so entfernen Sie entweder die Quell- oder Zielfestplatte aus dem Computer, bevor Sie diesen erneut starten. Anderenfalls wird das Betriebssystem von der ersten der beiden Festplatten starten und das Betriebssystem der zweiten Platte seine Bootfähigkeit verlieren." Das Kontrollkästchen **Computer nach dem Klonen ausschalten** hat den Fokus und ist automatisch deaktiviert.
2. Klicken Sie auf **Abschluss**, um die Aktion zur Liste der ausstehenden Aktionen hinzuzufügen.
3. Klicken Sie auf **Ausführen** in der Symbolleiste und dann **Fertig stellen** im Fenster **Ausstehende Aktionen**.
4. Warten Sie dann, bis die Aktion beendet ist.
5. Und danach, bis der Computer ausgeschaltet wird.
6. Entfernen Sie entweder die Quell- oder Zielfestplatte aus dem Computer.
7. Schalten Sie den Computer wieder ein.

Falls Sie die NT-Signatur bewahren müssen:

1. Entfernen Sie sofern nötig das Häkchen im Kontrollkästchen **NT-Signatur kopieren**.
2. Entfernen Sie sofern nötig das Häkchen im Kontrollkästchen **Computer nach dem Klonen ausschalten**.
3. Klicken Sie auf **Abschluss**, um die Aktion zur Liste der ausstehenden Aktionen hinzuzufügen.
4. Klicken Sie auf **Ausführen** in der Symbolleiste und dann **Fertig stellen** im Fenster **Ausstehende Aktionen**.
5. Warten Sie dann, bis die Aktion beendet ist.

10.6.3 Festplatten konvertieren: MBR zu GPT

In folgenden Fällen kann es angebracht sein, einen MBR- in einen GPT-Basisdatenträger zu konvertieren:

- Wenn Sie mehr als 4 primäre Laufwerke auf einem Laufwerk benötigen.
- Wenn Sie die Zuverlässigkeit der Festplatte gegen möglichen Datenverlust erhöhen müssen.

Wenn Sie einen MBR- in einen GPT-Basisdatenträger konvertieren müssen:

1. Bestimmen Sie den MBR-Basisdatenträger, der zu GPT konvertiert werden soll.
2. Rechtsklicken Sie auf das betreffende Laufwerk und wählen Sie dann **Zu GPT konvertieren** im Kontextmenü.

   Sie erhalten eine Warnmeldung, dass Sie im Begriff sind, von MBR nach GPT zu konvertieren.
3. Indem Sie auf **OK** klicken, fügen Sie MBR-zu-GPT-Konvertierung der Liste der ausstehenden Aktionen hinzu.

(Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausfьhren (S. 316). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

Beachten Sie: Ein GPT-partitioniertes Laufwerk reserviert am Ende des partitionierten Bereiches Speicherplatz für einen benötigten Backupbereich, in dem Kopien des GPT-Headers und der Partitionstabelle gespeichert werden. Sollte die Festplatte so voll sein, dass keine automatische Verringerung der Laufwerksgröße möglich ist, so wird die MBR-zu-GPT-Konvertierung fehlschlagen.

Die Aktion kann außerdem nicht rückgängig gemacht werden. Wenn Sie eine MBR-Festplatte mit einer primären Partition haben, diese erst zu GPT und dann wieder zurück zu MBR konvertieren, so wird die Partition zu einem logischen Laufwerk, welches dann nicht mehr als Systempartition verwendet werden kann.

Wenn Sie ein Betriebssystem installieren wollen, das GPT-Festplatten nicht unterstützt, so ist eine Rückkonvertierung der Festplatte zu MBR über dasselbe Menü möglich (der Befehl für diese Aktion lautet **Zu MBR konvertieren**).

Konvertierung dynamischer Datenträger: MBR zu GPT

Eine direkte MBR-zu-GPT-Konvertierung von dynamischen Datenträgern wird von Acronis Disk Director Lite nicht unterstützt. Sie können jedoch zum selben Ziel kommen, wenn Sie die folgenden Konvertierungen durchführen:

1. MBR Festplatten-Konvertierung: Dynamisch zu Basis (S. 308) unter Verwendung der Aktion **Zu Basis konvertieren**.
2. Konvertierung von Basisdatenträgern: MBR zu GPT durch Verwendung der Aktion **Zu GPT konvertieren**.
3. GPT Festplatten-Konvertierung: Basis zu Dynamisch (S. 307) durch Verwendung der Aktion **Zu Dynamisch konvertieren**.

10.6.4 Festplatten konvertieren: GPT zu MBR

Wenn Sie ein Betriebssystem installieren wollen, das GPT-Festplatten nicht unterstützt, so ist eine Konvertierung der GPT-Platte zu MBR möglich (der Befehl für diese Aktion lautet **Zu MBR konvertieren**).

Wenn Sie eine GPT-Festplatte zu MBR konvertieren müssen:

1. Bestimmen Sie die GPT-Festplatte, die zu MBR konvertiert werden soll.
2. Rechtsklicken Sie auf das betreffende Laufwerk und wählen Sie dann **Zu MBR konvertieren** im Kontextmenü.

   Sie erhalten eine Warnmeldung, dass Sie im Begriff sind, von GPT nach MBR zu konvertieren.

   Ihnen werden die Auswirkungen auf das System erläutert, wenn das gewählte Lafuwerk von GPT zu MBR konvertiert wird. Z.B., dass die Konvertierung bewirken kann, dass das System nicht mehr auf das Laufwerk zugreifen und somit auch das Betriebssystem nicht mehr starten kann – oder dass auf manche Volumes des gewählten GPT-Laufwerks im MBR-Modus nicht mehr zugegriffen werden kann (weil diese jenseits der 2 TByte-Grenze liegen).

   Beachten Sie, dass ein zu einer GPT-Festplatte gehörendes Laufwerk nach der irreversiblen Konvertierung zu einer logischen Partition wird.

3. Indem Sie auf **OK** klicken, fügen Sie die GPT-zu-MBR-Konvertierung der Liste der ausstehenden Aktionen hinzu.

(Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausfьhren (S. 316). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

10.6.5 Festplatten konvertieren: Basis zu Dynamisch

In folgenden Fällen ist eine Konvertierung von Basis- zu dynamischen Datenträgern angebracht:

- Wenn Sie die Festplatte als Teil einer dynamischen Laufwerksgruppe verwenden wollen.
- Wenn Sie eine erhöhte Zuverlässigkeit der Datenspeicherung auf der Festplatte erreichen wollen.

Wenn Sie einen Basis- zu einem dynamischen Datenträger konvertieren müssen:

1. Wählen Sie den zu konvertierenden Basisdatenträger.
2. Rechtsklicken Sie auf das betreffende Laufwerk und wählen Sie im Kontextmenü **Zu Dynamisch konvertieren**. Ihnen wird eine abschließende Warnung angezeigt, dass die Konvertierung von Basis zu Dynamisch ansteht.
3. Sobald Sie in dieser Warnmeldung auf **OK** klicken, wird die Konvertierung sofort durchgeführt und falls notwendig der Computer neu gestartet.

   Beachten Sie: Ein dynamischer Datenträger belegt das letzte Megabyte des physikalischen Laufwerks mit einer Datenbank, die eine so genannte Four-Level-Beschreibung (Volume-Component-Partition-Disk) für jedes dynamische Laufwerk enthält. Sollte sich während der Konvertierung zu Dynamisch herausstellen, dass der Basisdatenträger voll ist und daher die Laufwerksgröße nicht automatisch reduziert werden kann, so schlägt die Konvertierungsaktion fehl.

Sollten Sie irgendwann den dynamischen wieder zu einem Basisdatenträger zurückwandeln wollen, etwa um ein Betriebssystem zu verwenden, welches dynamische Datenträger nicht unterstützt, so können Sie dafür dasselbe Menü verwenden (wobei der Aktionsbefehl **Zu Basis konvertieren** lautet).

Konvertierung eines System-Laufwerkes

Acronis Disk Director Lite benötigt nach einer Basis-zu-Dynamisch-Konvertierung keinen Neustart des Betriebssystems, sofern:

1. Auf der Festplatte nur ein Betriebssystem vom Typ Windows Server 2008/Vista vorhanden ist.
2. Auf dem Computer dieses Betriebssystem läuft.

Die Konvertierung von 'Basis' zu 'Dynamisch' eines Laufwerks, das eine Systempartition enthält, benötigt einiges an Zeit – wobei jeder Stromausfall, jedes unbeabsichtigte Ausschalten oder versehentliche Drücken des Reset-Schalters während der Aktion den Verlust der Bootfähigkeit bewirken kann.

Anders als der Windows Disk Manager bewahrt das Programm die Bootfähigkeit eines **Offline-Betriebssystems** nach der Aktion.

10.6.6 Laufwerk konvertieren: Dynamisch zu Basis

Eine Rückkonvertierung von dynamischen zu Basis-Laufwerken ist z.B. dann angebracht, wenn Sie ein Betriebssystem verwenden wollen, dass dynamische Laufwerke nicht unterstützt.

Wenn Sie ein Laufwerk von 'Dynamisch' zu 'Basis' konvertieren müssen:

1. Wählen Sie das zu konvertierende dynamische Laufwerk.
2. Klicken Sie mit der rechten Maustaste auf das betreffende Laufwerk und wählen Sie im Kontextmenü **Zu 'Basis' konvertieren**. Ihnen wird eine abschließende Warnung angezeigt, dass die Konvertierung von Dynamisch zu Basis ansteht.

   Ihnen werden die Auswirkungen auf das System erläutert, wenn das gewählte Laufwerk vom Typ 'Dynamisch' zu 'Basis' konvertiert wird. Z. B. dass die Umwandlung bewirken kann, dass das System nicht mehr auf das Laufwerk zugreifen und somit auch ein Betriebssystem nicht mehr starten kann – oder dass Sie für den Fall, dass das zu konvertierende Laufwerke Volumes von einem Typ enthält, die nur von dynamischen Laufwerken unterstützt werden (alle Laufwerkstypen außer Volumes vom Typ 'Einfach') über den möglichen Verlust von Daten infolge der Konvertierung gewarnt werden.

   Beachten Sie, dass die Aktion nicht auf dynamische Laufwerke angewendet werden kann, die übergreifende, Stripeset- oder RAID-5-Volumes enthalten.

3. Sobald Sie in dieser Warnmeldung auf **OK** klicken, wird die Konvertierung sofort durchgeführt.

Nach der Umwandlung werden 8 MB des Laufwerksspeichers für zukünftige Konvertierungen von Basis zu Dynamisch reserviert.

Der resultierende nicht zugeordnete Speicherplatz und die anvisierte maximale Volume-Größe können von Fall zu Fall variieren (z.B. weil die Größe einer Spiegelung die Größe einer anderen Spiegelung bedingt oder weil die letzten 8 MB Speicherplatz für zukünftige Konvertierungen von 'Basis' zu 'Dynamisch' reserviert werden).

Systemlaufwerk konvertieren

Acronis Disk Director Lite benötigt nach einer Dynamisch-zu-Basis-Konvertierung keinen Neustart des Betriebssystems, sofern:

1. Auf dem Laufwerk ist nur ein Betriebssystem vom Typ Windows Server 2008/Vista installiert.
2. Die Maschine dieses Betriebssystem ausführt.

Die Dynamisch-zu-Basis-Konvertierung Festplatte, die eine Systempartition enthält, benötigt einiges an Zeit – wobei jeder Stromausfall, jedes unbeabsichtigte Ausschalten oder versehentliche Drücken des Reset-Schalters während der Aktion den Verlust der Bootfähigkeit bewirken kann.

Anders als der Windows Disk Manager gewährleistet das Programm:

- sichere Konvertierung eines dynamischen zu einem Basis-Laufwerk, sofern dieses Laufwerk Volumes **mit Daten** für einfache und gespiegelte Volumes enthält.

- in Multiboot-Systemen die Bootfähigkeit eines Systems, das während der Aktion **offline** war.

10.6.7 Laufwerkstatus ändern

Die Funktion 'Laufwerkstatus ändern' gilt für die Betriebssysteme Windows Vista SP1+, Windows Server 2008 und Windows 7 und bezieht sich auf die aktuelle Laufwerksstruktur (S. 301).

Der Laufwerksstatus erscheint immer in der grafischen Anzeige des Laufwerks neben dem Laufwerksnamen; es gibt folgende Möglichkeiten:

- **Online**

  Der Status 'online' bedeutet, dass auf das Laufwerk im Modus Lesen-Schreiben zugegriffen werden kann. Dies ist der normale Laufwerkstatus. Wenn das Laufwerk nur im Lesemodus verfügbar sein soll, wählen Sie das Laufwerk aus und ändern Sie den Status zu 'offline'; wählen Sie dazu **Disk-Status zu offline ändern** im Menü **Aktionen**.

- **Offline**

  Der Status 'offline' bedeutet, dass auf das Laufwerk nur im Lesemodus zugegriffen werden kann. Um den Modus des gewählten Laufwerks von offline zurück zu online zu ändern, wählen Sie **Disk-Status auf online ändern** im Menü **Aktionen**.
  Wenn ein Laufwerk den Status offline hat und der Laufwerkname als **Fehlend** angegeben ist, kann das Betriebssystem dieses Laufwerk nicht finden bzw. nicht identifizieren. Es ist möglicherweise defekt, getrennt oder abgeschaltet. Informationen darüber, wie Sie ein als fehlend und offline gekennzeichnetes Laufwerk wieder in den Status online bringen, finden Sie in diesem Artikel in der Microsoft Knowledge Base:
  http://technet.microsoft.com/de-de/library/cc732026%28WS.10%29.aspx.

10.7 Aktionen für Volumes

Acronis Disk Director Lite ermöglicht folgende auf Partitionen anwendbare Aktionen:

- Partition erstellen (S. 310) – erstellt neue Partitionen mit Hilfe des Assistenten zur Partitionserstellung
- Partition lцschen (S. 314) – löscht eine gewählte Partition
- Aktiv setzen (S. 314) – kennzeichnet eine gewählte Partition als „Aktiv“, so dass ein hier installiertes Betriebssystem gebootet werden kann.
- Laufwerksbuchstaben дndern (S. 315) – wechselt den Laufwerksbuchstaben der gewählten Partition
- Bezeichnung дndern (S. 315) – ändert die Datenträgerbezeichnung der gewählten Partition
- Volume formatieren (S. 316) – formatiert ein Volume mit einem benötigten Dateisystem

Die Vollversion des Acronis Disk Director verfügt über weitere Werkzeuge zum Arbeiten mit Partitionen.

Acronis Disk Director Lite benötigt einen exklusiven Zugriff auf die Zielpartition. Das bedeutet, dass dann auch kein anderes Laufwerksverwaltung-Werkzeug (etwa die Windows Datenträgerverwaltung) auf sie zugreifen kann. Sollten Sie eine Meldung erhalten, dass die Partition nicht blockiert werden kann, so schließen Sie das die Partition gerade benutzende Laufwerksverwaltung-Werkzeug und starten erneut. Schließen Sie alle aktiven Festplatten-Werkzeuge, sofern Sie nicht bestimmen können, welche Anwendung die Partition gerade blockiert.

10.7.1 Eine Partition erstellen

Beispiele, wann eine neue Partition benötigt wird:

- Wiederherstellung eines früher gesicherten Backups mit exakt derselben Konfiguration;
- separate Speicherung von Sammlungen ähnlicher Dateien – z.B. Sammlungen von MP3- oder Videodateien auf einer separaten Partition;
- Sicherung der Backups (Images) anderer Partitionen/Festplatten auf einem besonderen Laufwerk;
- Installation eines neuen Betriebssystems (oder einer Auslagerungsdatei) auf einer neuen Partition;
- Hinzufügen neuer Hardware zu einem Computer.

Das Werkzeug zum Erstellen neuer Partitionen in Acronis Disk Director Lite ist der **Assistent zur Partitionserstellung**.

10.7.1.1 Verschiedene Arten dynamischer Volumes

Einfaches Volume (Simple)

Ein Laufwerk, das vom freien Speicherplatz eines einzelnen physikalischen Laufwerks erstellt wurde. Es kann aus einer oder auch mehreren Regionen auf der Festplatte bestehen, die durch den „Logical Disk Manager“ (LDM) von Windows virtuell vereint werden. Es stellt keine zusätzlichen Vorteile bereit, weder bei der Geschwindigkeit noch bei der Größe.

Übergreifendes Volume (Spanned)

Ein Laufwerk, basierend auf dem freien Speicher mehrerer physikalischer Festplatten, die durch den LDM miteinander verbunden sind. Bis zu 32 Laufwerke können zu einen Volume integriert werden, was zwar einerseits Hardware-Größenbeschränkungen sprengt, aber andererseits auch bedingt, dass bei Ausfall nur eines Laufwerks die Gesamtheit aller Daten verloren geht und kein Teil dieses übergreifenden Laufwerkes entfernt werden kann, ohne dass das ganze Laufwerk zerstört wird. Daher bringt ein übergreifendes Volume weder eine bessere Zuverlässigkeit, noch eine bessere E/A-Rate.

Stripeset-Volume

Ein manchmal auch RAID-0 genanntes Laufwerk, das aus gleich großen „Daten-Stripesets“ besteht, die quer über alle verwendeten Laufwerke geschrieben werden; was bedeutet, dass Sie zur Erstellung eines Stripeset-Volumes zwei oder mehr dynamische Laufwerke benötigen. Die Laufwerke in einem Volume vom Typ 'Stripeset' müssen nicht identisch sein, aber auf jeder Laufwerk, das Sie in das Volume aufnehmen wollen, muss ungenutzter Speicher vorhanden sein und die Größe des Volumes wird bestimmt durch die Größe des kleinsten Speicherplatzes. Der Datenzugriff bei einem Volume vom Typ 'Stripeset' ist üblicherweise schneller als der vergleichbare Zugriff auf ein einziges physikalisches Laufwerk, weil die Eingabe/Ausgabe-Operationen über mehr als ein Laufwerk verteilt werden.

Laufwerke vom Typ 'Stripeset' werden zur Performance-Steigerung und nicht wegen besserer Zuverlässigkeit erstellt, da sie keine redundanten Informationen enthalten.

Gespiegeltes Volume (Mirrored)

Ein manchmal auch RAID-1 genannter, fehlertoleranter Laufwerkstyp, dessen Daten auf zwei identischen physikalischen Festplatten dupliziert werden. Alle Daten des einen Laufwerks werden zur Schaffung der Datenredundanz auf das andere Laufwerk kopiert. Nahezu jedes Laufwerk kann gespiegelt werden, einschließlich System- und Boot-Laufwerke – falls der Laufwerke ausfällt, kann immer noch auf die Daten des verbliebenen Laufwerks zugegriffen werden. Leider

gibt es starke Hardware-Begrenzungen bezüglich Größe und Geschwindigkeit bei der Verwendung von gespiegelten Volumes.

Gespiegeltes Stripeset-Volume

Ein auch RAID-1+0 genanntes, fehlertolerantes Volume, welches die Vorteile erhöhter E/A-Geschwindigkeit des Typs 'Stripeset' mit der Redundanz beim Typ 'Gespiegelt' kombiniert. Was jedoch bleibt, ist ein offensichtlicher, von der 'Spiegelung'-Architektur stammender Nachteil: ein schlechtes Laufwerk-zu-Volume-Größenverhältnis.

RAID-5

Ein fehlertolerantes Stripeset-Volume, dessen Daten über eine Zusammenstellung (Array) von drei oder noch mehr Laufwerken quer verteilt sind. Die Festplatten müssen nicht identisch sein, aber jede Festplatte des „Volumes“ muss über gleich große Blöcke an nicht zugeordnetem Speicherplatz verfügen. Außerdem werden über das Laufwerk-Array auch Paritätsdaten (speziell berechnete Werte, die im Fehlerfall zur Datenrekonstruktion verwendet werden können) verteilt gespeichert. Und diese Paritätsdaten werden immer auf einem anderen Laufwerk als die eigentlichen Daten gespeichert. Sollte eine physikalische Platte ausfallen, so kann der Anteil des RAID-5-Laufwerks, der auf dieser Festplatte lag, aus den verbliebenen Daten und den Paritätsdaten wiederhergestellt werden. Ein RAID-5-Volume bietet erhöhte Zuverlässigkeit und ermöglicht die Speicherbegrenzungen physikalischer Laufwerke zu überwinden, wobei das Disk-zu-Volume-Größenverhältnis besser ist als bei Laufwerken vom Typ 'Gespiegelt' (Mirrored).

10.7.1.2 Der Assistent zur Partitionserstellung

Der Assistent zur **Partitionserstellung** ermöglicht Ihnen, jeden Partitionstyp (inkl. System und Aktiv) anzulegen, ein Dateisystem zu wählen, einen Laufwerksbuchstaben zuzuweisen und noch weitere Laufwerksverwaltung-Funktionen zu verwenden.

Sie können Schritt für Schritt Aktionsparameter eingeben und jederzeit für Korrekturen auch wieder zu vorherigen Schritten zurückwechseln. Um Sie bei Ihrer Wahl zu unterstützen, ist jeder Parameter mit detaillierten Anweisungen ergänzt.

So erstellen Sie eine neue Partition:

Starten Sie den **Assistenten zur Partitionserstellung** durch Wahl des Befehls **Partition erstellen** im Seitenleistenbereich **Assistenten** – oder rechtsklicken Sie auf einen nicht zugeordneten Speicherplatz und wählen im erscheinenden Kontextmenü **Partition erstellen**.

Bestimmen Sie den zu erstellenden Partitionstyp

In diesem ersten Schritt müssen Sie die Art der Partition spezifizieren, die Sie erstellen wollen. Die folgenden Partitionstypen stehen zur Verfügung:

- Basis
- Einfach/Übergreifend
- Stripset
- Gespiegelt
- RAID-5

Ihnen wird eine kurze Beschreibung für jeden Partitionstyp angezeigt (zum besseren Verständnis der Vorteile und Beschränkungen jeder möglichen Partitionsarchitektur).

*Sollte das aktuelle, auf dem Computer installierte Betriebssystem den gewählten Partitionstyp nicht unterstützen, so erhalten Sie eine entsprechende Warnung. In diesem Fall wird die **Weiter**-Schaltfläche deaktiviert, so dass Sie zum Fortsetzen der Partitionserstellung einen anderen Partitionstyp wählen müssen.*

Durch Klicken der **Weiter**-Schaltfläche gelangen Sie zum nächsten Assistentenschritt: Ziellaufwerk wдhlen (S. 312).

Ziellaufwerk wählen

Der nächste Assistentenschritt fordert Sie auf, die Festplatte zu wählen, deren unzugeordneter Speicher für die Partitionserstellung genutzt wird.

So erstellen Sie ein Basis-Volume:

- Wählen Sie die Zielfestplatte und den nicht zugeordneten Speicherplatz, von dem die Basis-Volume erstellt werden soll.

So erstellen Sie eine einfaches/übergreifendes Volume:

- Wählen Sie eine oder mehrere Zielfestplatten, auf der/denen die Partition erstellt wird.

So erstellen Sie ein gespiegeltes Volume:

- Wählen Sie zwei Ziellaufwerke, auf denen das Volume erstellt wird.

So erstellen Sie eine Stripeset-Volume:

- Wählen Sie zwei oder mehr Ziellaufwerke, auf denen das Volume erstellt wird.

So erstellen Sie eine RAID-5-Partition:

- Wählen Sie drei Ziellaufwerke, auf denen das Volume erstellt wird.

Nach der Wahl der Laufwerke ermittelt der Assistent die maximale Größe des resultierenden Volumes, das sich aus der Menge des auf dem Laufwerk verfügbaren, nicht zugeordneten Speicherplatzes sowie gegebenen Anforderungen des zuvor bestimmten Volume-Typs ableitet.

Wenn Sie versuchen, ein **dynamisches** Laufwerk auf einem oder mehreren **Basisdatenträgern** anzulegen, so erhalten Sie eine Warnmeldung, dass die gewählten Festplatten automatisch zu dynamischen Datenträgern konvertiert werden.

Sofern erforderlich (abhängig vom gewählten Partitionstyp), werden Sie aufgefordert, Ihrer Auswahl eine notwendige Anzahl von Laufwerken hinzuzufügen.

Durch Verwendung der **Zurück**-Schaltfläche können Sie zu früheren Schritten des Assistenten wechseln: Partitionstyp festlegen (S. 311).

Durch Klicken der **Weiter**-Schaltfläche gelangen Sie zum nächsten Assistentenschritt: PartitionsgrцЯe festlegen (S. 312).

Partitionsgröße festlegen

Auf der dritten Assistentenseite können Sie die Größe der zukünftigen Partition definieren, abhängig von den zuvor gemachten Einstellungen. Um die benötigte Größe innerhalb der minimalen und maximalen Grenzen einzustellen, können Sie den Schieberegler verwenden oder die gewünschten Werte im Eingabefenster eintippen oder die Begrenzungslinien der grafischen Laufwerksdarstellung mit der Maus verschieben.

Bei Verwendung des maximalen Wertes wird normalerweise der gesamte nicht zugeordnete Speicherplatz in die Laufwerkserstellung eingeschlossen. Der resultierende nicht zugeordnete

Speicher und die anvisierte maximale Laufwerksgröße können von Fall zu Fall variieren (z.B. weil die Größe einer Mirror-Platte die Größe einer anderen Mirror-Platte bedingt oder weil auf der Festplatte die letzten 8 MB für zukünftige Konvertierungen von Basis zu Dynamisch reserviert werden).

Wenn bei Basis-Partitionen einiger nicht zugeordneter Speicherplatz auf der Festplatte verbleibt, so können Sie außerdem die Position der neuen Partition wählen.

Durch Verwendung der **Zurück**-Schaltfläche können Sie zu früheren Schritten des Assistenten wechseln: Ziellaufwerk wдhlen (S. 312).

Durch Klicken der **Weiter**-Schaltfläche gelangen Sie zum nächsten Assistentenschritt: Volume-Optionen einstellen (S. 313).

Volume-Optionen einstellen

Im nächsten Assistentenschritt können Sie einen **Laufwerksbuchstaben** zuweisen (Standard ist der erste freie Buchstabe im Alphabet) und optional die **Datenträgerbezeichnung** (Standard ist keine Bezeichnung). Hier spezifizieren Sie außerdem das **Dateisystem** und die **Clustergröße**.

Der Assistent fordert Sie auf, eines der Windows-Dateisysteme zu wählen: FAT16 (bei Partitionsgrößen über 2 GB deaktiviert), FAT32 (bei Partitionsgrößen über 2 TB deaktiviert), NTFS oder Sie lassen die Partition **Unformatiert**.

Bei Wahl der Clustergröße können Sie jede Zahl aus den für ein bestimmtes Dateisystem vorgegebenen Größen wählen. Beachten Sie, dass das Programm Ihnen schon die Clustergröße vorschlägt, die zum Volume und dem gewählten Dateisystem am besten passt.

Beim Erstellen einer Basis-Volume, die auch als System-Volume verwendet werden kann, offeriert der Assistent eine geänderte Anzeige mit der Möglichkeit, den **Partitionstyp** auf **Primär**, **Aktiv** oder **Logisch** einzustellen.

Primär ist die gängige Wahl, wenn ein Betriebssystem auf dem Volume installiert werden soll. Wählen Sie **Aktiv**, wenn Sie auf dem Volume ein Betriebssystem installieren wollen, von dem der Computer beim Start direkt bootet. Wenn die Einstellung **Primär** nicht ausgewählt ist, so ist auch die Option **Aktiv** ausgeschaltet. Soll das Volume nur zum Speichern von Daten verwendet werden, so wählen Sie **Logisch**.

*Ein Basisdatenträger kann bis zu vier primäre Volumes enthalten. Sollten diese schon existieren, so muss das Laufwerk zur Erstellung weiterer primärer Volumes in ein dynamisches Volume konvertiert werden – anderenfalls sind die Einstellungen **Aktiv** und **Primär** deaktiviert und Sie können nur den Volume-Typ **Logisch** wählen. Durch eine Warnmeldung werden Sie gegebenenfalls darauf hingewiesen, dass von diesem Volume nicht gebootet werden kann.*

*Wenn Sie für eine neue Datenträgerbezeichnung Ziffern verwenden, die vom aktuell installierten Betriebssystem nicht unterstützt werden, erhalten Sie auch eine Warnung und die **Weiter**-Schaltfläche wird deaktiviert. Sie müssen die Bezeichnung ändern, um mit der Erstellung des neuen Volumes fortzufahren.*

Durch Verwendung der **Zurück**-Schaltfläche können Sie zu früheren Schritten des Assistenten wechseln: PartitionsgrцЯe festlegen (S. 312).

Durch Klicken auf **Abschluss** wird die geplante Aktion abgeschlossen.

Zur Abarbeitung der geplanten Aktion klicken Sie zuerst auf **Ausführen** in der Symbolleiste und dann auf **Fertig stellen** im erscheinenden Fenster **Ausstehende Aktionen.**

Sollten Sie bei FAT16/FAT32 eine Clustergröße von 64K oder bei NTFS eine Größe von 8-64KB eingestellt haben, so kann Windows das Volume zwar mounten, aber bei manchen anderen Programmen (z.B. Setup-Programmen) kann es zu Fehlkalkulationen bei der Laufwerksgrößenberechnung kommen.

10.7.2 Volume löschen

Diese Version von Acronis Disk Director Lite hat eine reduzierte Funktionalität, weil sie hauptsächlich zur Vorbereitung fabrikneuer Systeme für die Wiederherstellung zuvor gesicherter Partitionsabbilder gedacht ist. Funktionen zur Größenänderung bestehender Partitionen und zur Erstellung neuer Partitionen unter Verwendung des Speicherplatzes bereits vorhandener Partitionen finden sich nur in der Vollversion, so dass mit der vorliegenden Lite-Version das Löschen von Partitionen manchmal der einzige Weg sein kann, um benötigten Festplattenplatz ohne Veränderung der Festplattenkonfiguration freizugeben.

Nachdem eine Partition gelöscht wurde, wird sie dem nicht zugeordneten Speicherplatz der Platte hinzugefügt. Das lässt sich nutzen, um eine neue Partition zu erstellen oder den Partitionstyp einer anderen zu verändern.

So löschen Sie eine Partition:

1. Wählen Sie eine Festplatte und auf dieser die zu löschende Partition.
2. Wählen Sie den Befehl **Partition löschen** oder einen entsprechenden Eintrag in der **Aktionen**-Liste der Seitenleiste – oder klicken Sie auf das Symbol **Partition löschen** in der Symbolleiste.

   Sollten sich auf der Partition Daten befinden, so werden Sie mit einer Meldung gewarnt, dass alle Informationen unwiederbringlich verloren gehen.

3. Indem Sie im Fenster **Partition löschen** auf **OK** klicken, wird der Befehl zur Liste ausstehender Aktionen hinzugefügt.

(Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausfьhren (S. 316). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

10.7.3 Die aktive Partition setzen

Wenn Sie über mehrere primäre Partitionen verfügen, so müssen Sie eine davon als Boot-Partition spezifizieren. Dafür können Sie die Partition so einstellen, dass sie „aktiv“ wird. Auf einer Festplatte kann jedoch nur ein Laufwerk aktiv sein: wird eine Partition neu als aktiv gesetzt, dann wird bei einer zuvor aktiven Partition die entsprechende Einstellung aufgehoben.

So setzen Sie eine Partition aktiv:

1. Bestimmen Sie eine primäre Partition auf einem MBR-Basisdatenträger, die aktiv gesetzt werden soll.
2. Rechtsklicken Sie auf das betreffende Laufwerk und wählen Sie im Kontextmenü **Aktiv setzen**.

   Sofern keine andere aktive Partition im System vorliegt, wird die Operation zur Liste der ausstehenden Aktionen hinzugefügt.

   Beachten Sie, dass sich durch das Aktivsetzen der neuen Partition wiederum der Laufwerksbuchstabe einer zuvor aktiven Partition ändern kann und daher installierte Anwendungsprogramme evtl. nicht mehr lauffähig sein können.

3. Sollte im System eine andere Partition aktiv sein, so erhalten Sie eine Warnmeldung, dass diese bisherige aktive Partition zuerst auf passiv gesetzt werden muss. Indem Sie im **Warndialog** auf **OK** klicken, wird das Setzen der aktiven Partition zur Liste ausstehender Aktionen hinzugefügt.

Beachten Sie: Selbst wenn ein Betriebssystem auf der neuen aktiven Partition liegt, kann es unter Umständen sein, dass der Computer dennoch nicht von ihr booten kann. Sie müssen Ihre Entscheidung bestätigen, damit die neue Partition als aktiv gesetzt wird.

(Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausfьhren (S. 316). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

Die neue Laufwerksstruktur wird sofort in der **Laufwerksverwaltung**-Ansicht angezeigt.

10.7.4 Laufwerksbuchstaben ändern

Das Windows-Betriebssystem weist Festplatten-Laufwerken ihre Laufwerksbuchstaben während des Startvorgangs zu. Diese Laufwerksbuchstaben werden vom Betriebssystem und Anwendungsprogrammen verwendet, um Dateien und Ordner auf den Partitionen zu finden.

Das Hinzufügen neuer Festplatten sowie das Erstellen oder Löschen von Partitionen auf existierenden Platten kann Ihre Systemkonfiguration ändern. Das kann zur Folge haben, dass manche Anwendungsprogramme nicht mehr normal funktionieren oder Benutzerdateien nicht mehr automatisch gefunden bzw. geöffnet werden können. Um dem entgegenzuwirken, können Sie vom Betriebssystem auf die Partitionen zugewiesene Laufwerksbuchstaben manuell ändern.

So ändern Sie den Laufwerksbuchstaben einer Partition, der vom Betriebssystem zugewiesen wurde:

1. Wählen Sie die Partition, deren Laufwerksbuchstabe geändert werden soll.
2. Rechtsklicken Sie auf das betreffende Laufwerk und wählen Sie im Kontextmenü **Laufwerksbuchstabe ändern**.
3. Wählen Sie im Dialog **Laufwerksbuchstabe ändern** den neuen Laufwerksbuchstaben.
4. Indem Sie im Fenster **Laufwerksbuchstabe ändern** auf **OK** klicken, wird der Befehl zur Liste ausstehender Aktionen hinzugefügt.

   (Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausfьhren (S. 316). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

Die neue Laufwerksstruktur wird sofort in der **Laufwerksverwaltung**-Ansicht angezeigt.

10.7.5 Volume-Bezeichnung ändern

Die Bezeichnung eines Volumes ist ein optionales Attribut. Es handelt sich um einen Namen, der dem Volume zur leichteren Erkennung zugeordnet wird. So kann z.B. ein Volume SYSTEM genannt werden (Volume für das Betriebssystem) oder PROGRAMME (Volume für Anwendungen) oder DATEN (Volume für Dokumente), was jedoch nicht bedeutet, dass auf diesem Volume nur noch Daten gespeichert werden können, die dieser Bezeichnung entsprechen.

Unter Windows werden die Volume-Bezeichnungen im Verzeichnisbaum des Explorers angezeigt: Laufwerk1(C:), Laufwerk2(D:), Laufwerk3(E:), etc. Laufwerk1, Laufwerk2 und Laufwerk3 sind Volume-Bezeichnungen. Eine Volume-Bezeichnung ist außerdem auch in den Öffnen-/Speichern-Dialogen aller Anwendungsprogramme sichtbar.

So ändern Sie die Bezeichnung eines Volumes:

1. Rechtsklicken Sie auf das gewünschte Volume und wählen Sie **Bezeichnung ändern**.
2. Geben Sie in das Textfeld des Dialoges **Bezeichnung ändern den neuen Laufwerksnamen ein.**
3. Indem Sie im Fenster **Bezeichnung ändern** auf **OK** klicken, wird der Befehl zur Liste ausstehender Aktionen hinzugefügt.

*Wenn Sie für die neue Bezeichnung des Volumes Zeichen verwenden, die vom aktuell installierten Betriebssystem nicht unterstützt werden, erhalten Sie eine Warnung und die **Weiter**-Schaltfläche wird deaktiviert. Um mit der Änderung der Volume-Bezeichnung fortfahren zu können, dürfen Sie für die Aktion nur noch unterstützte Zeichen verwenden.*

(Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausfьhren (S. 316). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

Die neue Bezeichnung wird sofort in der **Laufwerksverwaltung**-Ansicht angezeigt.

10.7.6 Volume formatieren

Fälle, in denen es angebracht sein kann, ein Volume mit einem neuen Dateisystem zu formatieren:

- Um zusätzlichen Speicherplatz zu gewinnen, der zuvor durch eine ungünstige Clustergröße auf FAT16- oder FAT32-Dateisystemen verloren ging.
- Um auf dem Volume befindliche Daten auf schnelle und relativ verlässliche Art zu zerstören

So formatieren Sie ein Volume:

1. Wählen Sie das zu formatierende Volume.
2. Klicken Sie mit der rechten Maustaste auf das betreffende Volume und wählen Sie im Kontextmenü **Formatieren**.

   Darauf erscheint das Fenster **Volume formatieren**, in dem Sie die Einstellungen für das neue Dateisystem vornehmen können. Sie können eines der Windows-Dateisysteme wählen: FAT16 (bei Volume-Größen über 2 GB deaktiviert), FAT32 (bei Volume-Größen über 2 TB deaktiviert) oder NTFS.

   Falls notwendig, können Sie im Textfeld für das Volume eine Bezeichnung eingeben: standardmäßig ist dieses Fenster leer.

   Bei Wahl der Clustergröße können Sie jede Zahl aus den für ein bestimmtes Dateisystem vorgegebenen Größen wählen. Beachten Sie, dass das Programm Ihnen schon die Clustergröße vorschlägt, die zum Volume und dem gewählten Dateisystem am besten passt.
3. Wenn Sie auf **OK** klicken, um mit dem Befehl **Volume formatieren** fortzufahren, wird dieser der Liste ausstehender Aktionen hinzugefügt.

   (Um die hinzugefügte Aktion zu vollenden, müssen Sie sie ausfьhren (S. 316). Wenn Sie das Programm ohne Ausführung der ausstehenden Aktionen beenden, werden diese alle verworfen.)

Die neue Volume-Struktur wird sofort in der **Laufwerksverwaltung**-Ansicht angezeigt.

Sollten Sie bei FAT16/FAT32 eine Clustergröße von 64K oder bei NTFS eine Größe von 8-64KB eingestellt haben, so kann Windows das Volume zwar mounten, aber bei manchen anderen Programmen (z.B. Setup-Programmen) kann es zu Fehlkalkulationen bei der Laufwerksgrößenberechnung kommen.

10.8 Ausstehende Aktionen

Alle vom Anwender manuell oder mit Hilfe eines Assistenten zusammengestellten Aktionen werden solange als ausstehend angesehen, bis der Anwender durch Anstoß eines entsprechenden Befehls bewirkt, dass alle Änderungen dauerhaft gemacht werden. Bis dahin visualisiert Acronis Disk Director Lite lediglich die neue Laufwerksstruktur so, wie es sich aus den geplanten, auf Laufwerken und Volumes anzuwendenden Aktionen ergibt. Dieser Ansatz ermöglicht geplante Aktionen zu kontrollieren, beabsichtigte Änderungen doppelt überprüfen zu können und sofern nötig Aktionen vor der Ausführung jederzeit abbrechen zu können.

Das Programm zeigt Ihnen also zuerst eine Liste aller ausstehenden Aktionen an, um Sie vor unbeabsichtigten Änderungen Ihrer Laufwerke zu bewahren.

Sie finden in der Anzeige **Laufwerksverwaltung** eine Symbolleiste, die Icons zum Starten der Befehle **Rückgängig**, **Wiederherstellen** und **Ausführen** enthält, welche speziell für die ausstehenden Aktionen gedacht sind. Sie können diese Befehle außerdem über das Menü **Disk ManagementLaufwerksverwaltung** der Konsole starten.

Alle geplanten Operationen werden zur Liste der ausstehenden Aktionen hinzugefügt.

Über den Befehl **Rückgängig** können Sie je den letzten Befehl in dieser Liste zurücksetzen. Solange die Liste nicht leer ist, steht dieser Befehl zur Verfügung.

Über den Befehl **Wiederherstellen** können Sie die letzte ausstehende und zuvor rückgängig gemachte Aktion wieder zurückholen.

Der Befehl **Ausführen** bringt Sie zum Fenster **Ausstehende Aktionen**, in dem Sie die Liste dieser ausstehenden Aktionen noch einmal einsehen können. Durch Klick auf **Fertig stellen** wird dann die Ausführung gestartet. Sobald Sie den Befehl **Fertig stellen** gewählt haben, sind Sie jedoch nicht mehr in der Lage, irgendeinen Befehl oder eine Aktion rückgängig zu machen. Sie können die Umsetzung aber vorher durch Klicken auf **Abbrechen** aufheben. In dem Fall werden an der Liste der ausstehenden Aktionen keine Veränderungen durchgeführt.

Da Acronis Disk Director Lite, wenn Sie das Programm ohne die ausstehenden Aktionen auszuführen beenden, alle Aktionen verwirft, erhalten Sie eine entsprechende Warnmeldung, wenn Sie das **Laufwerksverwaltung** einfach verlassen.

11 Anwendungen mit Laufwerk-Backups schützen

Dieser Abschnitt beschreibt, wie Sie ein Laufwerk-Backup verwenden, um auf Windows-Servern laufende Anwendungen zu schützen.

Diese Information gilt für physikalische und virtuelle Maschinen; und auch unabhängig davon, ob die virtuellen Maschinen auf Hypervisor-Ebene oder innerhalb eines Gast-Betriebssystems gesichert werden.

Laufwerk-Backups können eine VSS-kompatible Anwendung potenziell schützen, Acronis hat den Schutz jedoch für folgenden Anwendungen getestet:

- Microsoft Exchange Server
- Microsoft SQL Server
- Active Directory (Active Directory-Domänendienste)
- Microsoft SharePoint

Verwendung eines Laufwerk-Backups auf einem Anwendungsserver

Ein Laufwerk- bzw. Volume-Backup speichert das Dateisystem eines Laufwerks oder Volumes 'als Ganzes'. Daher speichert es alle zum Booten des Betriebssystems erforderlichen Informationen. Es speichert außerdem alle Anwendungsdateien, Datenbankdateien eingeschlossen. Sie können dieses Backup auf verschiedene Arten verwenden, abhängig von der Situation.

- Im Fall eines Desasters können Sie das komplette Laufwerk wiederherstellen, um sicherzustellen, dass das Betriebssytem und alle Anwendungen funktionieren und laufen.
- Sollte das Betriebssystem intakt sein, dann müssen Sie vielleicht eine Anwendungsdatenbank auf ein früheres Stadium zurücksetzen. Stellen Sie dafür die Datenbankdateien wieder her und verwenden Sie die systemeigenen Tools der Anwendung, damit die Datenbank von der Anwendung erkannt und verwendet wird.
- Sie müssen vielleicht nur ein bestimmtes Datenelement extrahieren, beispielsweise ein PDF-Dokument von einem Microsoft SharePoint Server-Backup. Sie können in diesem Fall ein Volume aus einem Backup an das Dateisystem des Anwendungsservers mounten und die systemeigenen Tools der Anwendung verwenden, um das Element zu extrahieren.

11.1 Backup eines Anwendungsservers

Um einen Anwendungsserver schützen zu können, erstellen Sie einen Backup-Plan oder verwenden Sie die Funktion **Backup jetzt** (wie im Abschnitt 'Backup (S. 58) beschrieben).

Anwendungen, die Datenbanken verwenden, erfordern einige einfache Maßnahmen, um die Konsistenz der Anwendungsdaten innerhalb eines Laufwerk-Backups sicherzustellen.

Backup kompletter Maschinen

Datenbanken können auf mehr als einem Laufwerk oder Volume gespeichert sein. Um sicherzustellen, dass alle benötigten Dateien in einem Backup enthalten sind, sollten Sie die komplette Maschine sichern. Das gewährleistet außerdem, dass die Anwendung weiterhin geschützt bleibt, wenn Sie noch mehr Datenbanken hinzufügen oder zukünftig die Protokolldateien verlagern.

Sollten Sie sicher sein, dass die Datenbanken und damit assoziierte Dateien immer auf denselben Volumes vorliegen, dann möchten Sie möglicherweise nur Backups dieser Volumes erstellen. Oder Sie möchten separate Backup-Pläne für das System-Volume und diejenigen Volumes erstellen,

welche die Daten speichern. Stellen Sie in beiden Fällen sicher, dass alle Volumes, die notwendige Dateien enthalten, in das Backup aufgenommen werden. Anweisungen darüber, wie Sie die Datenbankpfade ermitteln können, finden Sie im Abschnitt 'Datenbankdateien suchen (S. 320)'.

Sollten die Anwendungsdatenbanken sich auf mehreren Maschinen befinden, dann sichern Sie im Backup alle Maschinen mit derselben Planung. Schließen Sie beispielsweise alle SQL Server, die zu einer SharePoint-Farm gehören, in einen zentralen Backup-Plan ein, der nach einer festen Planung läuft.

Volume Shadow Copy (VSS) verwenden

Microsoft Volume Shadow Copy Service (VSS) sollte verwendet werden, um die Konsistenz der Datenbankdateien in einem Backup zu gewährleisten. Ohne VSS würden die Dateien in einem 'crash-konsistenten' Zustand sein; was bedeutet, dass das System nach der Wiederherstellung im gleichen Zustand wäre, als wäre beim Beginn des Backups die Stromversorgung getrennt worden. Während solche Backups für die meisten Anwendungen ausreichend sind, können Anwendungen, die Datenbanken verwenden, von einem 'crash-konsistenten' Zustand aus möglicherweise nicht starten.

Ein VSS Provider benachrichtigt alle VSS-kompatiblen Anwendungen, dass das Backup dabei ist zu starten. Das gewährleistet, dass alle Datenbanktransaktionen dann abgeschlossen sind, wenn Acronis Backup & Recovery 11.5 den Daten-Snapshot erfasst. Was wiederum den konsistenten Zustand der Datenbanken im resultierenden Backup sicherstellt.

Acronis Backup & Recovery 11.5 kann verschiedene VSS Provider verwenden. Bei Microsoft-Produkten ist der Microsoft Software Shadow Copy Provider (Microsoft-Softwareschattenkopie-Anbieter) die beste Wahl.

VSS auf einer physikalischen Maschine verwenden

Auf einer physikalischen Maschine ist die Verwendung von VSS konfigurierbar. Das gilt außerdem auch für eine virtuelle Maschine, deren Backup innerhalb des Gastbetriebssystems erfolgt. Sie müssen die Verwendung von VSS möglicherweise manuell aktivieren, falls die Werksvoreinstellung vom Standardwert geändert wurde.

Sie müssen außerdem sicherstellen, dass die VSS Writer für die entsprechende Anwendung angeschaltet wurden. Beim Windows Small Business Server 2003 ist der Exchange-Schreiber standardmäßig ausgeschaltet. Informationen zum Anschalten des Schreibers finden Sie im Microsoft Knowledge Base-Artikel http://support.microsoft.com/kb/838183/.

So aktivieren Sie die standardmäßige Verwendung von VSS für jeden auf einer Maschine erstellten Backup-Plan:

1. Verbinden Sie die Konsole mit der Maschine.
2. Wählen Sie im oberen Menü **Optionen** –> **Standardoptionen für Backup und Recovery** –> **Standardoptionen für Backup** –> **Volume Shadow Copy Service**.
3. Klicken Sie auf **Volume Shadow Copy Service verwenden**.
4. Klicken Sie in der Liste der **Snapshot-Provider** auf **Software – System-Provider**.

Wenn die Konsole mit dem Management Server verbunden ist, können Sie für alle registrierten Maschinen dieselben Standardeinstellungen festlegen.

VSS auf einer virtuellen Maschine verwenden

Beim Backup einer virtuellen Maschine auf Hypervisor-Ebene ist die Verwendung von VSS nicht konfigurierbar. VSS wird immer verwendet, falls die VMware Tools oder die Hyper-V-Integrationsdienste in einem entsprechenden Gast-System installiert sind.

Die Installation dieser Tools/Dienste ist eine allgemeine Voraussetzung für Backups auf Hypervisor-Ebene. Wenn Fehler wie 'stillgelegte Snapshots' (Quiesced Snapshot) beim Backup von virtuellen ESX(i)-Maschinen auftreten, hilft normalerweise ein Neuinstallieren oder ein Update der VMware Tools mit anschließendem Neustart der virtuellen Maschinen. Weitere Informationen finden Sie unter http://kb.acronis.com/content/4559.

Abschneiden von Transaktionsprotokollen

Active Directory verwendet normalerweise Umlaufprotokollierung. Die Protokolle von anderen VSS-kompatiblen Anwendungen (ausgenommen Microsoft SQL Server) können mithilfe der Option **VSS-Voll-Backup verwenden** (S. 142) abgeschnitten werden. Diese Option ist nur auf physikalischen und virtuellen Maschinen wirksam, auf denen der Agent für Windows installiert ist.

Andere verfügbare Lösungen beinhalten:

1. Manuelles Abschneiden der Protokolle oder durch Verwendung eines Skripts. Weitere Informationen finden Sie unter 'Abschneiden von Transaktionsprotokollen (S. 324)'
2. Bei Microsoft Exchange Server die Verwendung des dedizierten Agenten für Microsoft Exchange Server.
3. Für Microsoft SQL Server, unter Verwendung des Agenten für Microsoft SQL Server (Single-Pass).

Anwendungsspezifische Empfehlungen

Siehe 'Optimale Vorgehensweisen beim Backup von Anwendungsservern (S. 328)'.

11.1.1 Datenbankdateien suchen

Dieser Abschnitt beschreibt, wie Sie Anwendungsdatenbankdateien finden können.

Wir empfehlen, dass Sie die Datenbankdatei-Pfade ermitteln und diese dann an einem sicheren Platz speichern. Sie sparen sich damit Zeit und Aufwand, wenn Sie die Anwendungsdaten wiederherstellen wollen.

11.1.1.1 SQL Server-Datenbankdateien

SQL Server-Datenbanken haben drei Arten von Dateien:

- Primäre Datendateien – haben standardmäßig die Erweiterung **.mdf**. Jede Datenbank hat eine primäre Datendatei.
- Sekundäre Datendateien – haben standardmäßig die Erweiterung **.ndf**. Sekundäre Datendateien sind optional. Manche Datenbanken haben überhaupt keine, andere Datenbanken können dagegen mehrere sekundäre Datendateien haben.
- Protokolldateien – haben standardmäßig die Erweiterung **.ldf**. Jede Datenbank hat wenigstens eine Protokolldatei.

Stellen Sie sicher, dass alle Volumes, die irgendwelche der oberen Dateien enthalten, in das Backup aufgenommen werden. Falls Ihre Datenbanken beispielsweise im Verzeichnis 'C:\Programme\Microsoft SQL Server\MSSQL.1\MSSQL\Data\' vorliegen und die Protokolldateien aber im Verzeichnis 'F:\TLs\', dann müssen Sie beide Volumes (C:\ und F:\) im Backup sichern.

Die Pfade zu allen Datenbankdateien einer Instanz per Transact-SQL bestimmen

Das folgende Transact-SQL-Skript kann 'wie vorliegend' verwendet werden, um die Pfade zu allen Datenbankdateien einer Instanz zu ermitteln.


```
Create Table ##temp
(
    DatabaseName sysname,
    Name sysname,
    physical_name nvarchar(500),
    size decimal (18,2),
    FreeSpace decimal (18,2)
)
Exec sp_msforeachdb '
Use [?];
Insert Into ##temp (DatabaseName, Name, physical_name, Size, FreeSpace)
    Select DB_NAME() AS [DatabaseName], Name,  physical_name,
    Cast(Cast(Round(cast(size as decimal) * 8.0/1024.0,2) as decimal(18,2)) as
nvarchar) Size,
    Cast(Cast(Round(cast(size as decimal) * 8.0/1024.0,2) as decimal(18,2)) -
        Cast(FILEPROPERTY(name, ''SpaceUsed'') * 8.0/1024.0 as decimal(18,2)) as
nvarchar) As FreeSpace
    From sys.database_files'
Select * From ##temp
drop table ##temp
```

Die Speicherorte von Datenbankdateien per SQL Server Management Studio bestimmen

Standardspeicherorte

SQL Server-Datenbankdateien liegen in ihren Standardspeicherorten vor, sofern Sie die Pfade nicht manuell angepasst haben. So ermitteln Sie die Standardpfade von Datenbankdateien:

1. Führen Sie Microsoft SQL Server Management Studio aus und verbinden Sie sich mit der benötigten Instanz.
2. Klicken Sie mit der rechten Maustaste auf den Instanznamen und wählen Sie **Eigenschaften**.
3. Öffnen Sie die Seite **Datenbankeinstellungen** überprüfen Sie die im Bereich **Standardspeicherorte für Datenbank** angegebenen Pfade.

Benutzerdefinierte Speicherorte

Sollten die Speicherorte der SQL Server-Datenbankdateien angepasst worden sein, dann gehen Sie folgendermaßen vor:

1. Erweitern Sie im Microsoft SQL Server Management Studio die benötigte Instanz.
2. Klicken Sie mit der rechten Maustaste auf die Datenbank und wählen Sie **Eigenschaften**. Darauf öffnet sich das Dialogfenster **Datenbankeigenschaften**.
3. Klicken Sie im Fensterbereich **Seite auswählen** auf **Dateien** und überprüfen Sie die im Bereich **Datenbankdateien** angegebenen Pfade.

11.1.1.2 Exchange-Server-Datenbankdateien

Exchange-Datenbanken haben drei Arten von Dateien:

- **Datenbankdatei (.edb)**

  Enthält Nachrichtenköpfe, Nachrichtentext und Standardanhänge.

  Eine Exchange 2003/2007-Datenbank verwendet zwei Dateien: .edb für Textdaten und .stm für MIME-Daten.

- **Transaktionsprotokolldateien (.log)**

Enthält den Verlauf von an der Datenbank durchgeführten Änderungen. Erst nachdem eine Änderung sicher protokolliert wurde, wird diese dann auch in die Datenbankdatei geschrieben. Dieser Ansatz garantiert eine zuverlässige Wiederherstellung der Datenbank zu einem konsistenten Zustand, für den Fall, dass es zu einer plötzlichen Datenbankstörung kommt.

Die Größe jeder Protokolldatei beträgt 1024 KB (oder 5120 KB bei Exchange 2003) Sobald eine aktive Protokolldatei voll ist, schließt Exchange diese und erstellt eine neue Protokolldatei.

- **Prüfpunktdatei (.chk)**

  Verfolgt, wie weit Exchange damit fortgeschritten ist, protokollierte Informationen in die Datenbankdatei zu schreiben.

Gehen Sie folgendermaßen vor, um die Datenbankdatei- und Protokolldatei-Pfade herauszufinden.

Exchange 2010

Führen Sie mit der Exchange-Verwaltungsshell folgende Befehle aus:

```
Get-MailboxDatabase | Format-List -Property Name, EdbFilePath, LogFolderPath
```

Exchange 2007

Führen Sie mit der Exchange-Verwaltungsshell folgende Befehle aus:

- So rufen Sie die Datenbank-Pfade ab:

  ```
  Get-MailboxDatabase | Format-List -Property Name, EdbFilePath, StorageGroup
  ```

- So rufen Sie die Protokolldatei-Pfade ab:

  ```
  Get-MailboxDatabase | ForEach { Get-StorageGroup $_.StorageGroupName | Format-List
  -Property Name, LogFolderPath }
  ```

Exchange 2003

1. Starten Sie den Exchange-System-Manager.
2. Klicken Sie auf **Administrative Gruppen**.

   ***Anmerkung**: Sollten die administrativen Gruppen nicht erscheinen, dann sind sie möglicherweise nicht angeschaltet. Klicken Sie mit der rechten Maustaste zum Anschalten der administrativen Gruppen auf **Exchange-Organisation** und dann auf **Eigenschaften**. Klicken Sie, um das Kontrollkästchen 'Administrative Gruppen anzeigen' zu aktivieren.*

3. Gehen Sie folgendermaßen vor, um den Transaktionsprotokoll-Speicherort zu ermitteln:
   a. Klicken Sie mit der rechten Maustaste auf die Speichergruppe und wählen Sie **Eigenschaften**.
   b. Auf der Registerkarte **Allgemein** wird der Transaktionsprotokoll-Speicherort angezeigt.
4. Gehen Sie folgendermaßen vor, um den Datenbankdatei-Speicherort (für *.edb-Dateien) zu ermitteln:
   a. Erweitern Sie die benötigte Speichergruppe
   b. Klicken Sie mit der rechten Maustaste auf die Datenbank und wählen Sie **Eigenschaften**.
   c. Sie sehen in der Registerkarte **Datenbank** den Speicherort der Datenbankdatei und der Datenbank-Streamingdatei.

11.1.1.3 Active Directory-Datenbankdateien

Eine Active Directory-Datenbank besteht aus folgenden Dateien:

1. **NTDS.dit** (Datenbankdatei)
2. **Edb.chk** (Prüfpunktdatei)

3. **Edb*.log** (Transaktionsprotokolle)
4. **Res1.log** und **Res2.log** (zwei Reserveprotokolldateien)

Die Dateien befinden sich typischerweise im Ordner **%systemroot%\NTDS** (beispielsweise C:\Windows\NTDS) eines Domain-Controllers. Ihr Speicherort ist jedoch konfigurierbar. Die Datenbankdateien und die Transaktionsprotokolle können auf unterschiedlichen Volumes gespeichert werden. Stellen Sie sicher, dass beide Volume in das Backup aufgenommen werden.

Um den aktuellen Speicherort der Datenbankdateien und Transaktionsprotokolle bestimmen zu können, müssen Sie die Werte **DSA Database file** und **Database log files path** in folgenden Registry-Schlüsseln überprüfen:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
```

11.1.1.4 SharePoint-Datenbankdateien

SharePoint speichert Inhalte, Hilfsdaten der SharePoint-Dienste und die Farmkonfiguration in Microsoft SQL Server-Datenbanken.

So finden Sie Datenbankdateien in SharePoint 2010 (oder höher)

1. Öffnen Sie die Seite **Zentraladministration**.
2. Wählen Sie **Upgrade und Migration** –> **Datenbankstatus überprüfen**. Ihnen werden die SQL-Instanz und die Datenbanknamen für alle Datenbanken angezeigt.
3. Verwenden Sie Microsoft SQL Server Management Studio, um die Dateien der benötigten Datenbank zu identifizieren. Detaillierte Anweisungen finden Sie im Abschnitt SQL Server-Datenbankdateien (S. 320).

So finden Sie Inhaltsdatenbankdateien in SharePoint 2007

1. Öffnen Sie die Seite **Zentraladministration**.
2. Wählen Sie **Anwendungsmanagement** –> **Inhaltsdatenbanken**.
3. Wählen Sie eine Webapplikation.
4. Wählen Sie eine Datenbank. Sie sehen in der geöffneten Seite den Datenbankserver und den Datenbanknamen. Notieren Sie diese oder kopieren Sie die Information in eine Textdatei.
5. Wiederholen Sie Schritt 4 für andere Datenbanken der Webapplikation.
6. Wiederholen Sie die Schritte 3-5 für andere Webapplikationen.
7. Verwenden Sie Microsoft SQL Server Management Studio, um die Datenbankdateien zu identifizieren. Detaillierte Anweisungen finden Sie im Abschnitt SQL Server-Datenbankdateien (S. 320).

So finden Sie Konfigurations- oder Dienstdatenbankdateien in SharePoint 2007

1. Öffnen Sie die Seite **Zentraladministration**.
2. Wählen Sie **Anwendungsmanagement** –> **Gemeinsame Dienste dieser Farm erstellen oder konfigurieren**.
3. Klicken Sie mit der rechten Maustaste auf einen Anbieter für gemeinsame Dienste (Shared Services Provider) und wählen Sie **Eigenschaften bearbeiten**. Sie sehen in der geöffneten Seite den Datenbankserver und den Datenbanknamen. Notieren Sie diese oder kopieren Sie die Information in eine Textdatei.
4. Wiederholen Sie Schritt 3 für andere Anbieter für gemeinsame Dienste.
5. Verwenden Sie Microsoft SQL Server Management Studio, um die Datenbankdateien zu identifizieren. Detaillierte Anweisungen finden Sie im Abschnitt SQL Server-Datenbankdateien (S. 320).

11.1.2 Abschneiden von Transaktionsprotokollen

Dieser Abschnitt beschreibt, wie Sie Transaktionsprotokolle abschneiden können, wenn Sie Microsoft Exchange Server und Microsoft SQL Server mithilfe von Laufwerk-Backups schützen.

Die Empfehlungen für SQL Server gelten auch für SQL Server, die in einer Microsoft SharePoint-Farm enthalten sind. Active Directory-Datenbanken verwenden normalerweise Umlaufprotokollierung, daher benötigen Sie kein Abschneiden von Transaktionsprotokollen.

11.1.2.1 Abschneiden des Transkationsprotokolls und Verkleinern der Protokolldatei für SQL Server

Acronis Backup & Recovery 11.5 schneidet Transaktionsprotokolle nach Erstellung eines Laufwerk-Backups nicht ab. Falls Sie nicht die systemeigene Backup-Engine des Microsoft SQL Servers verwenden (oder die Backup-Lösung eines anderen Drittherstellers, die Transaktionsprotokolle automatisch verwaltet), dann können Sie die Protokolle mit folgenden Methoden verwalten.

- **Abschneiden des Transaktionsprotokolls**. Das Protokollabschneiden macht inaktive virtuelle Protokolldateien (die nur inaktive Protokolldatensätze enthalten) frei zur Wiederverwendung durch neue Protokolldatensätze. Abschneiden kann eine physikalische Protokolldatei daran hindern zu wachsen, aber dadurch wird nicht ihre Größe reduziert.

  Weitere Informationen über das Abschneiden finden Sie in folgendem Artikel: http://technet.microsoft.com/de-de/library/ms189085(v=sql.105)
- **Verkleinern der Protokolldatei**. Das Verkeinern einer Protokolldatei reduziert die physikalische Größe einer Protokolldatei, indem inaktive virtuelle Protokolldateien entfernt werden. Das Verkleinern ist am wirksamsten nach einer Protokollabschneidung.

  Weitere Informationen über das Verkleinern finden Sie in folgendem Artikel: http://technet.microsoft.com/de-de/library/ms178037(v=sql.105)

Protokollabschneidung durch SQL Server Management Studio

Wenn Sie eine Datenbank auf das einfache Wiederherstellungsmodell (Simple Recovery Model) umschalten, werden die Transaktionsprotokolle automatisch abgeschnitten.

1. So schalten Sie die Datenbank auf das einfache Wiederherstellungsmodell um:
   a. Führen Sie Microsoft SQL Server Management Studio aus und verbinden Sie sich mit der Instanz.
   b. Klicken Sie mit der rechten Maustaste auf die Datenbank und wählen Sie **Eigenschaften**. Darauf öffnet sich das Dialogfenster **Datenbankeigenschaften**.
   c. Klicken Sie im Fensterbereich **Seite auswählen** auf **Optionen**.
   d. Wählen Sie im Listenfeld **Wiederherstellungsmodell** das Modell **Einfach**.
2. Die Transaktionsprotokolldateien werden automatisch abgeschnitten.
3. Schalten Sie die Datenbank, auf gleiche Art wie in Schritt 1, zurück zum vollständigen oder massenprotokollierten Wiederherstellungsmodell.

Protokollabschneidung und -verkleinerung automatisieren

Sie können die obere Prozedur des Abschneidens mit einem Skript automatisieren und (optional) auch das Protokolldatei-Verkleinern hinzufügen. Falls Sie das Skript zu den 'Nach-Backup'-Befehlen (S. 135) hinzufügen, werden die Protokolle direkt nach einem Backup abgeschnitten und verkleinert. Bei dieser Methode wird angenommen, dass Sie über Kenntnisse zur Erstellung/Nutzung von Transact-SQL-Skripten verfügen und sich mit dem Utility **`sqlcmd`** auskennen.

Weitere Informationen über Transact-SQL und **sqlcmd** finden Sie in folgenden Artikeln:

- Transact-SQL verwenden: http://technet.microsoft.com/de-de/library/ms189826(v=sql.90)
- Das Utility **sqlcmd** verwenden: http://technet.microsoft.com/de-de/library/ms170572(SQL.90).aspx

So automatisieren Sie das Abschneiden und Verkleinern des Transaktionsprotokolls für eine SQL-Instanz

1. Erstellen Sie durch Verwendung des folgenden Templates ein Skript, welches die Protokolldateien für die Datenbanken der folgenden Instanz abschneidet und verkleinert:

   ```
   USE database_name
   ALTER DATABASE database_name SET RECOVERY SIMPLE;
   DBCC SHRINKFILE(logfile_name);
   ALTER DATABASE database_name SET RECOVERY FULL;
   ```

   Im letzten String hängt der Wert **SET RECOVERY** vom ursprünglichen Wiederherstellungsmodell der bestimmten Datenbank ab und kann **FULL** (vollständig) oder **BULK_LOGGED** (massenprotokolliert) sein.

   Beispiel für eine Instanz, die zwei Datenbanken (TestDB1 und TestDB2) hat:

   ```
   USE TestDB1;
   ALTER DATABASE TestDB1 SET RECOVERY SIMPLE;
   DBCC SHRINKFILE(TestDB1_log);
   ALTER DATABASE TestDB1 SET RECOVERY FULL;

   USE TestDB2;
   ALTER DATABASE TestDB2 SET RECOVERY SIMPLE;
   DBCC SHRINKFILE(TestDB2_log);
   ALTER DATABASE TestDB2 SET RECOVERY BULK_LOGGED;
   ```

2. Fügen Sie den nachfolgenden **sqlcmd**-Befehl dem 'Nach-Backup'-Befehl (S. 135) hinzu:

   ```
   sqlcmd -S myServer\instanceName -i C:\myScript.sql
   ```

   Dabei ist:

   - `myServer` – der Name des Servers
   - `instanceName` – der Name der Instanz
   - `C:\myScript.sql` – der Pfad zur in Schritt 1 erstellten Skriptdatei.

So automatisieren Sie das Abschneiden und Verkleinern des Transaktionsprotokolls für mehrere SQL-Instanzen

Falls Sie mehr als eine Instanz auf der Maschine haben und Sie die obere Prozedur auf diese Instanzen anwenden wollen, dann gehen Sie folgendermaßen vor.

1. Erstellen Sie eine separate Skriptdatei für jede Instanz (z. B. C:\script1.sql und C:\script2.sql).
2. Erstellen Sie eine Batchdatei (z.B. C:\truncate.bat), welche die Befehle für die korrespondierende Instanz enthält:

   ```
   sqlcmd -S myServer\instance1 -i C:\script1.sql
   sqlcmd -S myServer\instance2 -i C:\script2.sql
   ```

3. Spezifizieren Sie bei 'Nach-Backup-Befehl' den Pfad zu dieser Batchdatei.

11.1.2.2 Abschneiden des Transaktionsprotokolls für Exchange-Server

Über Microsoft Exchange-Server-Protokolle

Bevor eine Transaktion auf eine Datenbankdatei ausgeführt wird, protokolliert Exchange diese in eine Transaktionsprotokolldatei. Um zu verfolgen, welche der protokollierten Transaktionen auf die

Datenbank angewendet wurden, verwendet Exchange Prüfpunktdateien. Sobald die Transaktionen auf die Datenbank angewendet und per Prüfpunktdateien verfolgt wurden, werden die Protokolldateien nicht mehr länger von der Datenbank benötigt.

Werden die Protokolldateien nicht gelöscht, können diese möglicherweise den kompletten verfügbaren Speicherplatz belegen – und die Exchange-Datenbanken werden offline genommen, bis die Protokolldateien vom Laufwerk entfernt wurden. Die Verwendung von Umlaufprotokollierung ist nicht die bewährteste Methode für eine Produktionsumgebung. Bei aktivierter Umlaufprotokollierung überschreibt Exchange die erste Protokolldatei, nachdem deren Daten auf die Datenbank angewendet wurden – wodurch Sie nur Daten bis zum letzten Backup wiederherstellen können.

Wir empfehlen, dass Sie die Protokolldateien nach dem Backup eines Exchange-Servers löschen, weil Protokolldateien zusammen mit anderen Dateien gesichert werden. Sie können die Datenbank nach einer Wiederherstellung daher vorwärts und rückwärts 'rollen'.

Weitere Informationen über die Transaktionsprotokollierung finden Sie unter http://technet.microsoft.com/de-de/library/bb331958.aspx.

Protokollabschneidung unter Verwendung der Option VSS-Voll-Backup aktivieren

Die einfachste Methode der Protokollabschneidung ist die Verwendung der Backup-Option **VSS-Voll-Backup aktivieren** (S. 142) (**Optionen** –> **Standardoptionen für Backup und Recovery** –> **Standardoptionen für Backup** –> **Volume Shadow Copy Service** –> **VSS-Voll-Backup aktivieren**). Sie wird in den meisten Fällen empfohlen.

Sollte eine Aktivierung dieser Option unerwünscht sein (weil Sie beispielsweise die Protokolle einer anderen VSS-kompatiblen Anwendung bewahren müssen), dann folgen Sie den unteren Empfehlungen.

Abschneiden von Offline-Datenbanken protokollieren

Nach einem normalen Herunterfahren wird der Datenbankzustand als konsistent angesehen und die Datenbankdateien sind eigenständig (self-contained). Das bedeutet, dass Sie alle Protokolldateien der Datenbank oder Speichergruppe löschen können.

So löschen Sie Transaktionsprotokolldateien:

1. Trennen Sie die Datenbank (bei Exchange 2010) oder alle Datenbanken der Speichergruppe (bei Exchange 2003/2007). Zu weiteren Informationen, siehe:
   - Exchange 2010: http://technet.microsoft.com/de-de/library/bb123903
   - Exchange 2007: http://technet.microsoft.com/de-de/library/bb124936(v=exchg.80)
   - Exchange 2003: http://technet.microsoft.com/de-de/library/aa996179(v=exchg.65)
2. Löschen Sie alle Protokolldateien der Datenbank oder der Speichergruppe.
3. Mounten Sie die getrennte(n) Datenbank oder Datenbanken.

   Zu weiteren Informationen, siehe:
   - Exchange 2010: http://technet.microsoft.com/de-de/library/bb123587.aspx
   - Exchange 2007: http://technet.microsoft.com/de-de/library/aa998871(v=exchg.80).aspx
   - Exchange 2003: http://technet.microsoft.com/de-de/library/aa995829(v=exchg.65)

Abschneiden von Online-Datenbanken protokollieren

Diese Methode ist gut für Datenbanken, die permanent verwendet werden und daher nicht getrennt werden können. Wenn sich eine Datenbank in Verwendung befindet, können Sie nur solche

Transaktionsprotokolldateien sichern löschen, deren Daten auf die Datenbank angewendet wurden. Löschen Sie keine Protokolldateien, deren Daten nicht auf die Datenbank angewendet wurden; sie sind essentiell, um die Datenbank-Konsistenz bei unerwartetem Herunterfahren wiederherstellen zu können.

So löschen Sie angewendete Transaktionsprotokolle

1. Bestimmen Sie mit dem Tool **Eseutil**, welche Protokolle auf die Datenbank angewendet wurden:
   a. Führen Sie den Befehl **eseutil /mk <**Pfad zur Prüfpunktdatei**>** aus, wobei **<**Pfad zur Prüfpunktdatei**>** der Pfad zu der Prüfpunktdatei für die benötigte Datenbank oder Speichergruppe ist.
   b. Überprüfen Sie das Feld **Checkpoint** in der Anzeige. Sie sollten etwas sehen, das etwa so aussieht:

   ```
   CheckPoint: (0x60B, 7DF, 1C9)
   ```

   Die erste Zahl 0x60B ist die hexadezimale Protokollgenerierungsnummer der aktuellen Protokolldatei. Das bedeutet, dass alle Protokolldateien mit kleineren Zahlen auf die Datenbank angewendet wurden.
2. Löschen Sie alle Protokolldateien, deren Zahlen kleiner sind als die Zahl der aktuellen Protokolldatei. Sie können beispielsweise die Dateien Enn0000060A.log, Enn00000609.log (und niedrigere Dateien) sicher löschen.

Abschneiden nach einem Backup protokollieren

Sie können die obere Prozedur des Abschneidens mit einem Skript automatisieren. Falls Sie das Skript zu den 'Nach-Backup'-Befehlen (S. 135) hinzufügen, werden die Protokolle direkt nach einem Backup abgeschnitten.

Bei dieser Methode wird angenommen, dass Sie über Kenntnisse zur Erstellung/Nutzung von Skripten verfügen und sich mit dem Befehlszeilenwerkzeug von Acronis Backup & Recovery 11.5 auskennen (**acrocmd**). Weitere Informationen zu **acrocmd** finden Sie in der Befehlszeilen-Referenz.

Das Skript sollte folgende Schritte enthalten:

1. Mounten Sie die Volumes, die die benötigten Datenbankdateien enthalten, durch Verwendung des Befehls **mount**.

   Template:

   ```
   acrocmd mount --loc=<Pfad> --credentials=<Benutzername>,<password>
   --arc=<Archivname> --volume=<Volume-Nummern> --letter=<Laufwerksbuchstaben>
   ```

   Beispiel:

   ```
   acrocmd mount --loc=\\bkpsrv\backups --credentials=user1,pass1 --arc=my_arc
   --volume=1-1 --letter=Z
   ```

2. Bestimmen Sie in den gemounteten Volumes mit dem Tool **Eseutil**, welche Protokolle auf die Datenbank angewendet wurden. Diese Prozedur ist im Schritt 1 des oberen Abschnitts 'Abschneiden von Online-Datenbanken protokollieren' beschrieben.
3. Löschen Sie in der entsprechenden Online-Datenbank oder Speichergruppe alle Protokolldateien, deren Zahlen niedriger sind, als die Zahl der aktuellen Protokolldatei im Backup.
4. Trennen Sie die gemounteten Volumes durch Verwendung des Befehls **umount**.

11.1.3 Optimale Vorgehensweisen beim Backup von Anwendungsservern

11.1.3.1 Exchange-Server-Backup

Falls Sie nicht Microsoft Exchange Server 2010 SP2 verwenden, wird empfohlen, dass Sie die Konsistenz von Exchange-Datenbankdateien regelmäßig überprüfen.

In Exchange wird die Konsistenzprüfung mit dem Tool bzw. Befehl **Eseutil /K** durchgeführt. Dabei wird die Seitenebenenintegrität (Page-Level Integrity) von allen Exchange-Datenbanken und die Prüfsummen aller Datenbankseiten und Protokolldateien verifiziert. Der Überprüfungsvorgang kann zeitaufwendig sein. Weitere Informationen über die Verwendung von **Eseutil /K** finden Sie unter: http://technet.microsoft.com/de-de/library/bb123956(v=exchg.80).

Sie können die Konsistenzprüfung vor oder nach einem Backup durchführen.

- **Vor einem Backup**. Das gewährleistet, dass Sie keine beschädigten Echange-Datenbankdateien per Backup sichern.
  a. Trennen Sie die Datenbanken.
  b. Führen Sie **Eseutil /K** aus und überprüfen Sie die Ergebnisse der Verifizierung.
  c. Sollten die Datenbanken konsistent sein, dann mounten Sie sie erneut und führen Sie das Backup aus. Reparieren Sie anderenfalls die beschädigten Datenbanken.

  Weitere Informationen über Mounten und Trennen (Dismounten) von Datenbanken finden Sie im Abschnitt 'Abschneiden des Transaktionsprotokolls für Exchange-Server (S. 325)'.
- **Nach einem Backup**. Der Vorteil dieser Methode ist, dass Sie keine permanent verwendeten Datenbanken trennen müssen. Die Konsistenzprüfung im Backup ist jedoch viel langsamer als die Konsistenzprüfung von auf dem Laufwerk liegenden Datenbanken.

  Mounten (S. 276) Sie die Volumes (welche die benötigten Datenbankdateien enthalten) von dem Laufwerk-Backup im 'Nur Lesen'-Modus und führen Sie dann **Eseutil /K** aus.

  Sollte eine Prüfsummen-Inkonsistenz oder ein beschädigter Datei-Header gefunden werden, dann reparieren Sie die beschädigten Datenbanken und führen Sie das Backup erneut aus.

Tipp: *Acronis hat ein dediziertes Produkt zum Backup von Microsoft Exchange im Angebot – Acronis Backup & Recovery 11.5 für Microsoft Exchange Server. Wenn Sie dieses Produkt verwenden, überprüft der Agent für Exchange automatisch die Konsistenz von zu sichernden Datenbanken und überspringt Datenbanken mit Prüfsummen-Inkonsistenz oder beschädigtem Datei-Header. Im Gegensatz zu diesem Agenten verifiziert* ***Eseutil /K*** *die Seiten aller Exchange-Datenbanken, die auf dem Server vorhanden sind.*

11.1.3.2 Active Directory-Backup

Die Active Directory-Dienste verwenden eine Datenbank, die sich auf dem Dateisystem eines Domain-Controllers befindet. Falls die Domain zwei oder mehr Domain-Controller hat, werden die in der Datenbank gespeicherten Informationen kontinuierlich zwischen den Controllern repliziert.

Zu sichernde Volumes

Erstellen Sie Backups folgender Volumes eines Domain-Controllers, um ein Active Directory zu sichern:

- Das System-Volume und das Boot-Volume
- Die Volumes, auf denen sich die Active Directory-Datenbank und Transaktionsprotokolle (S. 322) befinden

- Das Volume mit dem Ordner SYSVOL. Der Standardort für dieses Verzeichnis ist **%SystemRoot%\SYSVOL**. Untersuchen Sie, um den aktuellen Speicherort dieses Ordners zu ermitteln, den **Sysvol**-Wert in folgendem Registry-Schlüssel:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
```

Weitere Überlegungen zum Backup

Stellen Sie bei der Einrichtung und Durchführung von Active Directory-Backups sicher, dass:

- Die Häufigkeit der Backup-Durchführung ist **mindestens monatlich.** Sollte Ihre Domain nur einen Domain-Controller haben, dann empfehlen wir eine mindestens tägliche Backup-Erstellung.
- Ihr aktuellstes Backup ist **nicht älter als die Hälfte der Tombstone-Lebensdauer.** Abhängig vom Betriebssystem, auf der Ihre Domain erstellt wurde, beträgt die vorgegebene Tombstone-Lebensdauer 60 oder 180 Tage. Es ist nicht wichtig, ob das letzte Backup vollständig oder inkrementell ist, denn Sie können erfolgreiche Wiederherstellungen von beiden ausführen.
- Sie können ein **zusätzliches Backup bei einem der folgenden Ereignisse** erstellen:
  - Die Active Directory-Datenbank und/oder Transaktionsprotokolle wurden zu einem anderen Speicherort verschoben.
  - Das Betriebssystem auf dem Domain-Controller wurde per Upgrade aktualisiert oder es wurde ein Service Pack installiert.
  - Es wurde ein Hotfix installiert, welches die Active Directory-Datenbank ändert.
  - Die Tombstone-Lebensdauer wurde administrativ geändert.

  Der Grund für dieses zusätzliche Backup ist, dass eine erfolgreiche Wiederherstellung des Active Directory von früheren Backups evtl. nicht mehr möglich ist.

11.1.3.3 SharePoint-Daten-Backup

Eine Microsoft SharePoint-Farm besteht aus Front-End-Webservern und Microsoft SQL Servern.

Ein Front-End-Webserver ist ein Host, auf dem SharePoint-Dienste laufen. Einige Front-End-Webserver können zueinander identisch sein (beispielswiese Front-End-Webserver, die einen Webserver ausführen). Sie müssen keine identischen Front-End-Webserver per Backup sichern, sondern nur individuelle.

Sie müssen, um SharePoint-Datenbanken sichern zu können, alle Microsoft SQL Servers und alle individuellen, zu der Farm gehörenden Front-End-Webserver per Backup sichern. Das Backup sollte mit *derselben Planung* durchgeführt werden. Das ist notwendig, weil die Konfigurationsdatenbank mit anderen Datenbanken synchronisiert werden muss. Falls beispielsweise die Inhaltsdatenbank Daten über eine Website enthält, während das letzte Backup der Konfigurationsdatenbank dies nicht tut, dann wird die Website nach Wiederherstellung der Konfigurationsdatenbank verwaist sein.

Falls Sie eine Advanced-Edition von Acronis Backup & Recovery 11.5 haben, ist der einfachste Weg, Backups einer SharePoint-Farm zu erstellen, entweder einen zentralen Backup-Plan zu erstellen (wie im Abschnitt 'Erstellung eines zentralen Backup-Plans (S. 396)' beschrieben) – oder die Funktion **Backup jetzt** zu verwenden (wie im Abschnitt 'Backup jetzt (S. 395)' beschrieben). Bei den Standalone-Editionen von Acronis Backup & Recovery 11.5 müssen Sie dieselbe Planung bei Erstellung eines Backup-Plans (S. 58) für jeden zur Farm gehörenden Server spezifizieren.

11.2 Wiederherstellung von SQL Server-Daten

Bei einem Desaster können Sie einen kompletten SQL Server dadurch wiederherstellen, dass Sie all seine Laufwerke von einem Laufwerk-Backup wiederherstellen. Sollten Sie den im Abschnitt 'Backup

eines Anwendungsservers (S. 318)' aufgeführten Empfehlungen gefolgt sein, dann sind alle SQL Server-Dienste funktionell und laufen, ohne dass weitere Aktionen notwendig sind. Die Server-Daten werden auf das Stadium zurückgesetzt, die zum Zeitpunkt des Backups gehabt haben.

Falls Sie eine gesicherte Datenbank zurück in die Produktion bringen müssen, dann stellen Sie die Datenbankdateien aus einem Laufwerk-Backup wieder her. Weitere Details finden Sie unter 'Wiederherstellung von SQL Server-Datenbankdateien von einem Laufwerk-Backup (S. 330)'.

Sollten Sie nur einen temporären Zugriff auf die gesicherten Datenbanken benötigen (zur Datengewinnung oder Datenextraktion), dann mounten Sie ein Laufwerk-Backup und greifen Sie auf die erforderlichen Daten zu. Weitere Details finden Sie unter 'Zugriff auf SQL Server-Datenbanken von einem Laufwerk-Backup aus (S. 331)'.

11.2.1 Wiederherstellung von SQL Server-Datenbanken von einem Laufwerk-Backup

Dieser Abschnitt beschreibt, wie Sie SQL Server-Datenbanken von einem Laufwerk-Backup ausgehend wiederherstellen können.

Anweisungen darüber, wie Sie die Datenbankpfade ermitteln können, finden Sie im Abschnitt 'SQL Server-Datenbankdateien (S. 320)'.

So stellen Sie SQL Server-Datenbanken wieder her

1. Verbinden Sie die Konsole mit der Maschine, auf der Sie die Aktion durchführen werden.
2. Gehen Sie zu dem Depot, welches das Laufwerk-Backup mit den SQL Server-Datenbankdateien enthält.
3. Klicken Sie auf Registerkarte **Datenanzeige**. Klicken Sie in der Liste **Anzeigen** auf **Ordner/Dateien**.
4. Wählen Sie die benötigten SQL Server-Datenbankdateien und klicken Sie auf **Recovery**. Die Daten werden standardmäßig auf den Zustand des letzten Backups zurückgesetzt. Verwenden Sie die Liste **Versionen**, falls Sie einen anderen Zeitpunkt wählen wollen, auf den die Daten zurückgesetzt werden sollen.
5. Auf der Recovery-Seite, unter dem Bereich **Recovery-Quelle**:
    a. Wählen Sie bei **Datenpfade** den Punkt **Benutzerdefiniert**.
    b. Spezifizieren Sie bei **Durchsuchen** einen Ordner, wohin die Dateien wiederhergestellt werden sollen.

        ***Anmerkung**: Wir empfehlen, dass Sie die SQL Server-Datenbankdateien zu einem lokalen Ordner des SQL Servers wiederherstellen, da alle SQL Server-Versionen vor SQL Server 2012 keine Datenbanken untertstützen, die auf Netzwerkfreigaben liegen.*

    c. Belassen Sie die übrigen Einstellungen wie vorliegend und klicken Sie dann auf **OK**, um dem Recovery-Task fortzufahren.
6. Fügen Sie die Datenbank nach Abschluss der Wiederherstellung so an, wie im Abschnitt 'SQL Server-Datenbanken anfügen (S. 331)' beschrieben.

    Details: Sollte Sie aus irgendeinem Grund nicht alle SQL Server-Datenbankdateien wiederhergestellt haben, dann können Sie die Datenbank nicht anfügen. Das Microsoft SQL Server Management Studio informiert Sie jedoch über alle Pfade und Namen der fehlenden Dateien und hilft Ihnen dabei zu identifizieren, aus welchen konkreten Dateien die Datenbank besteht.

11.2.2 Zugriff auf SQL Server-Datenbanken von einem Laufwerk-Backup aus

Falls Sie zur Datengewinnung oder aus anderen, kurzfristigen Gründen auf die SQL Server-Datenbanken zugreifen wollen, können Sie statt einer Wiederherstellung die Aktion **Image mounten** verwenden. Mounten Sie einfach die entsprechenden Volumes (die die benötigten Datenbankdateien enthalten) von einem Laufwerk-Backup (Image) im 'Lese/Schreib'-Modus und Sie können Datenbanken anfügen, Datenbankdateien ändern und mit diesen arbeiten, als würden Sie sich auf einem physikalischen Laufwerk befinden.

Sie können Volumes mounten, falls das Laufwerk-Backup in einem lokalen Ordner (ausgenommen optische Medien wie CDs, DVDs oder Blu-ray-Medien), in der Acronis Secure Zone oder auf einer Netzwerkfreigabe gespeichert vorliegt.

Anfügen von Datenbanken an einen SQL Server, die in einem Laufwerk-Backup enthalten sind

1. Verbinden Sie die Konsole mit dem SQL Server, auf dem der Agent für Windows installiert ist.
2. Wählen Sie im Hauptmenü die Befehle **Aktionen** –> **Image mounten**.
3. Wählen Sie im Bereich **Zu mountendes Image** das Quellarchiv und spezifizieren Sie das Backup.
4. Im Bereich **Mount-Einstellungen**:
   a. Wählen Sie bei **Mounten für** die Option **Alle Benutzer dieser Maschine**.
   b. Wählen Sie ein oder mehrere Volumes, welche die SQL Server-Datenbankdateien enthalten. Anweisungen darüber, wie Sie die Datenbankpfade ermitteln können, finden Sie im Abschnitt 'SQL Server-Datenbankdateien (S. 320)'.
   c. Wählen Sie den Zugriffsmodus **Lesen/Schreiben**.
   d. Spezifizieren Sie Laufwerksbuchstaben, die den gemounteten Volumes zugewiesen werden.
5. Verwenden Sie nach dem Mounten der Volumes die Anweisungen aus dem Abschnitt 'SQL Server-Datenbanken anfügen (S. 331)', um die Datenbanken direkt von den gemounteten Volumes aus anzufügen.
6. Führen Sie die gewünschten Aktionen mit den neu angefügten Datenbanken durch.
7. Trennen Sie die Datenbanken wieder von der Instanz, nachdem Sie die gewünschten Aktionen abgeschlossen haben, indem Sie Microsoft SQL Server Management Studio verwenden. Klicken Sie dazu mit der rechten Maustaste auf die Datenbank und wählen Sie **Aufgaben** –> **Trennen**.
8. Trennen Sie die gemounteten Volumes:
   a. Wählen Sie im Hauptmenü die Befehle **Navigation** –> **Gemountete Images**.
   b. Wählen Sie das Image und klicken Sie auf **Trennen**.

   Details: Acronis Backup & Recovery 11.5 erstellt beim Mounten eines Images im 'Lese/Schreib'-Modus ein neues inkrementelles Backup. Wir empfehlen, dieses inkrementelle Backup zu löschen.

11.2.3 SQL Server-Datenbanken anfügen

Dieser Abschnitt beschreibt, wie Sie eine Datenbank im SQL Server mithilfe des SQL Server Management Studios anfügen können. Es kann immer nur eine Datenbank gleichzeitig angefügt werden.

Das Anfügen einer Datenbank erfordert eine der folgenden Berechtigungen: **Datenbank erstellen**, **Beliebige Datenbank erstellen** oder **Beliebige Datenbank ändern**. Normalerweise verfügt auf der Instanz die Rolle **SysAdmin** über diese Berechtigungen.

So fügen Sie eine Datenbank an

1. Führen Sie Microsoft SQL Server Management Studio aus.
2. Verbinden Sie sich mit der benötigten SQL Server-Instanz und erweitern Sie dann die Instanz.
3. Klicken Sie mit der rechten Maustaste auf **Datenbanken** und klicken Sie dann auf **Anfügen**.
4. Klicken Sie auf **Hinzufügen**.
5. Lokalisieren und Wählen Sie im Dialogfenster **Datenbankdateien suchen** die .mdf-Datei der Datenbank.
6. Stellen Sie im Bereich **Datenbankdetails** sicher, dass die restlichen Datenbankdateien (.ndf- und .ldf-Dateien) gefunden werden.

   Details: SQL Server-Datenbankdateien werden möglicherweise nicht automatisch gefunden, falls:

   - Sie sich nicht am Standardspeicherort befinden – oder sie nicht im selben Ordner wie die primäre Datenbankdatei (.mdf) sind.Lösung: Spezifizieren Sie den Pfad zu den benötigten Dateien manuell in der Spalte **Aktueller Dateipfad**.
   - Sie haben einen unvollständigen Satz an Dateien wiederhergestellt, der die Datenbank bildet. Lösung: Stellen Sie die fehlenden SQL Server-Datenbankdateien aus dem Backup wieder her.
7. Klicken Sie, wenn alle Dateien gefunden sind, auf **OK**.

11.3 Wiederherstellung von Exchange-Server-Daten

Bei einem Desaster können Sie einen kompletten Exchange-Server dadurch wiederherstellen, dass Sie all seine Laufwerke von einem Laufwerk-Backup wiederherstellen. Sollten Sie den im Abschnitt 'Backup eines Anwendungsservers (S. 318)' aufgeführten Empfehlungen gefolgt sein, dann sind alle Exchange-Server-Dienste funktionell und laufen, ohne dass weitere Aktionen notwendig sind. Die Server-Daten werden auf das Stadium zurückgesetzt, die zum Zeitpunkt des Backups gehabt haben.

Durch Verwendung von Acronis Backup & Recovery 11.5 können Sie Exchange-Datenbankdateien von einem Laufwerk-Backup wiederherstellen. Mounten Sie eine Datenbank, um Sie wieder online zu bringen. Weitere Details finden Sie unter 'Mounten von Exchange-Server-Datenbanken (S. 333)'.

Falls Sie eine granuläre Wiederherstellung einzelner Postfächer (oder von in diesen enthaltenen Elementen) durchführen müssen, dann mounten Sie die wiederhergestellte Datenbank entweder als Wiederherstellungsdatenbank (Recovery Database, RDB) bei Exchange 2010 – oder als Speichergruppe für die Wiederherstellung (Recovery Storage Group, RSG) bei Exchange 2003/2007. Weitere Details finden Sie im Abschnitt 'Granuläres Recovery von Postfächern (S. 333)'.

11.3.1 Wiederherstellung von Exchange-Server-Datenbankdateien von einem Laufwerk-Backup

Dieser Abschnitt beschreibt die Verwendung von Acronis Backup & Recovery 11.5 zur Wiederherstellung von Exchange-Server-Datenbankdateien von einem Laufwerk-Backup.

Anweisungen darüber, wie Sie die Datenbankpfade ermitteln können, finden Sie im Abschnitt 'Exchange-Server-Datenbankdateien (S. 321)'.

So stellen Sie Exchange-Server-Datenbanken wieder her

1. Verbinden Sie die Konsole mit der Maschine, auf der Sie die Aktion durchführen werden.
2. Gehen Sie zu dem Depot, welches das Laufwerk-Backup mit den Exchange-Datendateien enthält.
3. Klicken Sie auf Registerkarte **Datenanzeige**. Klicken Sie in der Liste **Anzeigen** auf **Ordner/Dateien**.

4. Wählen Sie die benötigten Exchange-Datenbankdateien und klicken Sie auf **Recovery**. Die Daten werden standardmäßig auf den Zustand des letzten Backups zurückgesetzt. Verwenden Sie die Liste **Versionen**, falls Sie einen anderen Zeitpunkt wählen wollen, auf den die Daten zurückgesetzt werden sollen.
5. Auf der Recovery-Seite, unter dem Bereich **Recovery-Quelle**:
   a. Wählen Sie bei **Datenpfade** den Punkt **Benutzerdefiniert**.
   b. Spezifizieren Sie bei **Durchsuchen** einen Ordner, wohin die Datenbankdateien wiederhergestellt werden sollen.
6. Belassen Sie die übrigen Einstellungen wie vorliegend und klicken Sie dann auf **OK**, um dem Recovery-Task fortzufahren.

11.3.2 Mounten von Exchange-Server-Datenbanken

Sie können die Datenbanken nach Wiederherstellung der Datenbankdateien dadurch wieder online bringen, dass Sie sie mounten. Das Mounten wird mithilfe der Exchange-Verwaltungskonsole, dem Exchange-System-Manager oder der Exchange-Verwaltungsshell durchgeführt.

Die wiederhergestellte Datenbank wird sich im Stadium 'Dirty Shutdown' befinden. Eine Datenbank, die sich im Zustand 'Dirty Shutdown' befindet, kann vom System gemountet werden, falls sie zu ihrem ursprünglichen Speicherort wiederhergestellt wurde (vorausgesetzt, die Information über die ursprüngliche Datenbank ist im Active Directory vorhanden). Wenn Sie eine Datenbank zu einem anderen Speicherort wiederherstellen (beispielsweise eine neue Datenbank oder die Wiederherstellungsdatenbank), dann kann die Datenbank solange gemountet werden, bis Sie sie mithilfe des Befehls **`Eseutil /r <Enn>`** in das Stadium 'Clean Shutdown' bringen. **`<Enn>`** gibt das Protokolldatei-Präfix für die Datenbank an (bzw. die Speichergruppe, welche die Datenbank enthält), auf die Sie die Transaktionsprotokolldateien anwenden müssen.

Das Konto, welches Sie zum Anfügen einer Datenbank verwenden, muss an eine Exchange-Server-Administratorrolle und an eine lokalen Administratorengruppe des Zielservers delegiert sein.

Weitere Details zum Mounten von Datenbanken finden Sie in folgenden Artikeln:

- Exchange 2010: http://technet.microsoft.com/de-de/library/aa998871.aspx
- Exchange 2007: http://technet.microsoft.com/de-de/library/aa998871(v=EXCHG.80).aspx
- Exchange 2003: http://technet.microsoft.com/de-de/library/bb124040.aspx

11.3.3 Granuläres Recovery von Postfächern

Eine RDB (RSG) ist eine spezielle, administrative Datenbank (Speichergruppe) im Exchange-Server. Sie ermöglicht Ihnen, Daten aus einer gemounteten Postfach-Datenbank zu extrahieren. Die extrahierten Daten können zu existierenden Postfächern kopiert bzw. mit diesen zusammengeführt werden, ohne Benutzerzugriffe auf aktuelle Daten zu stören.

Weitere Informationen über RDB und RSG finden Sie in folgenden Artikeln:

- Exchange 2010: http://technet.microsoft.com/de-de/library/dd876954
- Exchange 2007: http://technet.microsoft.com/de-de/library/bb124039(v=exchg.80)
- Exchange 2003: http://technet.microsoft.com/de-de/library/bb123631(v=exchg.65)

So stellen Sie ein Postfach wieder her

1. Sollte keine RDB/RSG vorhanden sein, dann erstellen Sie diese, wie in folgenden Artikeln beschrieben:

- Exchange 2010: http://technet.microsoft.com/de-de/library/ee332321
- Exchange 2007: http://technet.microsoft.com/de-de/library/aa997694(v=exchg.80)
- Exchange 2003: http://technet.microsoft.com/de-de/library/bb124427(v=exchg.65)

2. Stellen Sie die Datenbankdateien in die RDB/RSG-Ordnerstruktur wieder her. Weitere Informationen über die Wiederherstellung von Datenbankdateien finden Sie im Abschnitt 'Wiederherstellung von Exchange-Server-Datenbankdateien von einem Laufwerk-Backup (S. 332)'.
3. Mounten Sie die Wiederherstellungsdatenbank. Weitere Informationen über das Mounten von Datenbanken finden Sie im Abschnitt 'Mounten von Exchange-Server-Datenbanken (S. 333)'.
4. Fahren Sie wie in folgenden Artikeln beschrieben fort:
   - Exchange 2010: http://technet.microsoft.com/de-de/library/ee332351
   - Exchange 2007: http://technet.microsoft.com/de-de/library/aa997694(v=exchg.80)
   - Exchange 2003: http://technet.microsoft.com/de-de/library/aa998109(v=exchg.65)

11.4 Wiederherstellung von Active Directory-Daten

Eine Active Directory-Wiederherstellung ist unterschiedlich, abhängig vom erforderlichen Wiederherstellungstyp.

Dieser Abschnitt betrachtet folgende Desaster-Szenarien:

- Ein Domain-Controller ist ausgefallen, aber andere Domain-Controller sind immer noch verfügbar. Siehe 'Wiederherstellung eines Domain-Controllers (andere DC sind verfügbar)'.
- Alle Domain-Controller sind ausgefallen (oder es gab nur einen). Siehe 'Wiederherstellung eines Domain-Controllers (keine anderen DC sind verfügbar)'.
- Die Active Directory-Datenbank ist beschädigt und der Active Directory-Dienst startet nicht. Siehe 'Wiederherstellung der Active Directory-Datenbank.
- Bestimmte Informationen wurden versehentlich aus dem Active Directory gelöscht. Siehe 'Wiederherstellung versehentlich gelöschter Informationen'.

11.4.1 Wiederherstellung eines Domain-Controllers (andere DC sind verfügbar)

Wenn einer von mehreren Domain-Controllern (DCs) ausgefallen ist, ist der Active Directory-Dienst immer noch verfügbar. Daher werden andere Domain-Controller Daten enthalten, die neuer sind als die Daten im Backup.

In diesem Fall wird üblicherweise ein Typ von Wiederherstellung durchgeführt, der als *nicht autorisierte Wiederherstellung* bekannt ist. Nicht autorisierte Wiederherstellung bedeutet, dass die Wiederherstellung den aktuellen Status des Active Directorys nicht beeinflusst.

Auszuführende Schritte

Falls die Domain noch andere Domain-Controller hat, können Sie eine nicht autorisierte Wiederherstellung eines ausgefallenen Domain-Controllers auf eine der folgenden Arten durchführen:

- **Wiederherstellung eines Domain-Controllers** von einem Backup mithilfe eines bootfähigen Mediums. Stellen Sie sicher, dass es kein USN-Rollback-Problem (S. 338) gibt.

- **Neuerstellung eines Domain-Controllers**, indem Sie das Betriebssystem installieren und die Maschine zu einem neuen Domain-Controller machen (durch Verwendung des Tools `dcpromo.exe`).

Auf beide Aktionen folgt eine automatische *Replikation*. Die Replikation bringt die Domain-Controller-Datenbank auf den neuesten Stand. Stellen Sie einfach nur sicher, dass der Active Directory-Dienst erfolgreich gestartet wurde. Sobald die Replikation abgeschlossen ist, ist der Domain-Controller aktuell und läuft wieder.

Wiederherstellung versus Neuerstellung

Neuerstellung erfordert nicht die Verfügbarkeit eines Backups. Eine Wiederherstellung ist normalerweise schneller als eine Neuerstellung. Eine Wiederherstellung ist jedoch in folgenden Fällen nicht möglich:

- Alle verfügbaren Backups sind älter als die 'Tombstone-Lebensdauer'. Tombstones werden während der Replikation verwendet, um sicherzustellen, dass ein auf einem Domain-Controller gelöschtest Objekt auch auf einem anderen Domain-Controller gelöscht wird. Eine korrekte Replikation ist daher nicht möglich, nachdem die Tombstones gelöscht wurden.
- Der Domain-Controller hatte eine Rolle für 'flexible einfache Mastervorgänge' (Flexible Single Master Operations, FSMO) inne – und Sie haben diese Rolle einem anderen Domain-Controller zugewiesen (Übernahme der Rolle). In diesem Fall würde eine Wiederherstellung des Domain-Controllers dazu führen, dass zwei Domain-Controller dieselbe FSMO-Rolle innerhalb der Domain innehaben und einen Konflikt verursachen.

Wiederherstellung eines Domain-Controllers, der eine FSMO-Rolle innehält.

Einige Domain-Controller halten eindeutige Rollen, die auch als 'flexible einfache Mastervorgänge'-Rollen (Flexible Single Master Operations roles, FSMO roles) oder Betriebsmaster-Funktionen (Operations Manager-Rollen) bekannt sind. Eine Beschreibung der FSMO-Rollen und ihres Umfangs (domänenweit oder gesamtstrukturweit) finden Sie im Microsoft Hilfe- und Support-Artikel http://support.microsoft.com/kb/324801.

Vor Neuerstellung eines Domain-Controllers, der eine PDC-Emulator-Rolle innehielt, müssen Sie diese Rolle übernehmen. Anderenfalls werden Sie nicht in der Lage sein, den neuerstellten Domain-Controller der Domain hinzuzufügen. Sie können nach der Neuerstellung des Domain-Controllers diese Rolle rückübertragen. Weitere Information zum Übernehmen und Übertragen von FSMO-Rollen finden Sie im Microsoft Hilfe- und Support-Artikel http://support.microsoft.com/kb/255504.

Um einzusehen, welche FSMO-Rollen welchem Domain-Controller zugewiesen sind, können Sie sich mit jedem aktuellen (live) Domain-Controller verbinden, indem Sie das Tool **`Ntdsutil`** verwenden, wie es im Microsoft Hilfe- und Support-Artikel http://support.microsoft.com/kb/234790 beschrieben ist. Folgen Sie den Schritten, die im Abschnitt 'Verwenden des Programms NTDSUTIL' des Artikels beschrieben sind:

- Folgen Sie bei den Betriebssystemen Windows 2000 Server und Windows Server 2003 allen Schritten wie angegeben.
- Bei den Windows Server 2008-Betriebssystemen müssen Sie in dem Schritt, indem Sie aufgefordert werden, **Domänenverwaltung** einzugeben, stattdessen **Rollen** eingeben. Folgen Sie den anderen Schritten wie angegeben.

11.4.2 Wiederherstellung eines Domain-Controllers (keine anderen DC sind verfügbar)

Sollten alle Domain-Controller ausgefallen sein, dann wird die nicht autorisierte Wiederherstellung tatsächlich zu einer autorisierten: die aus dem Backup wiederhergestellten Objekte sind dann die neuesten, die verfügbar sind. Eine Replikation von Active Directory-Daten kann nicht stattfinden, weil es keine aktuellen (live) Domain-Controller gibt. Das bedeutet:

- Nach dem Backup durchgeführte Änderungen am Active Directory gehen verloren.
- Eine Neuerstellung des Domain-Controllers ist keine Option.
- Sogar ein Backup mit einer abgelaufenen Tombstone-Lebensdauer kann verwendet werden.

Sie müssen die Volumes wiederherstellen, in denen die Active Directory-Datenbankdateien (S. 322) gespeichert sind. Sollten in diesen Volumes weitere, wichtige Daten (außer dem Active Directory) gespeichert sein, dann kopieren Sie diese Daten vor der Wiederherstellung zu einem anderen Speicherort.

So stellen Sie einen Domain-Controller wieder her, wenn keine anderen Domain-Controller verfügbar sind

1. Stellen Sie sicher, dass das neueste Backup für die Wiederherstellung verwendet wird. Das ist wichtig, weil alle nach dem Backup am Active Directory durchgeführten Änderungen verlorengehen werden.
2. Stellen Sie den Domain-Controller von dem Backup wieder her, indem Sie ein bootfähiges Medium verwenden.
3. Starten Sie den Domain-Controller neu. Stellen Sie sicher, dass der Active Directory-Dienst erfolgreich gestartet wurde.

11.4.3 Wiederherstellung der Active Directory-Datenbank

Sollten die Active Directory-Datenbankdateien beschädigt sein, der Domain-Controller aber noch im normalen Modus starten können, dann können Sie die Datenbank mit einer der folgenden Möglichkeiten wiederherstellen.

Höherstufen des Domain-Controllers

Bei dieser Art der Wiederherstellung ist die Datenbank nur dann verfügbar, falls die Domain noch andere Domain-Controller hat. Die Verfügbarkeit eines Backups ist nicht erforderlich.

Verwenden Sie zur Wiederherstellung der Datenbank das Tool **Dcpromo**, um den Domain-Controller mit der beschädigten Datenbank tieferzustufen – und dann, um diesen Domain-Controler anschließend wieder höherzustufen.

Fühlen Sie folgende Befehle aus, um den Domain-Controller erneut höherzustufen:

```
dcpromo /forceremoval

dcpromo /adv
```

Wiederherstellung der Datenbank von einem Backup

Bei dieser Art der Wiederherstellung kann die Datenbank unabhängig davon verwendet werden, ob die Domain noch weitere Domain-Controller hat.

Stellen Sie die Active Directory-Datenbankdateien (S. 322) wieder her, um die Datenbank wiederherzustellen. Falls Sie zusätzlich seit dem Backup irgendwelche Änderungen an den

Gruppenrichtlinienobjekten (GPOs) gemacht haben, müssen Sie außerdem den SYSVOL-Ordner (S. 328) wiederherstellen.

So stellen Sie die Active Directory-Datenbank von einem Backup aus wieder her

1. Starten Sie den Domain-Controller neu und drücken Sie während des Startvorgangs auf F8.
2. Wählen Sie im Fenster **Erweiterte Startoptionen** das Element **Verzeichnisdienst-Wiederherstellungsmodus**.
3. [Optional] Erstellen Sie eine Kopie der aktuellen Active Directory-Datenbankdatei, um die Änderungen bei Bedarf wieder rückgängig machen zu können.
4. Ändern Sie das ursprüngliche Konto des Acronis Agent Service auf das Administratorkonto des Verzeichnisdienst-Wiederherstellungsmodus (Directory Services Restore Mode, DSRM).
   a. Öffnen Sie das Snap-in **Dienste**.
   b. Klicken Sie in der Liste der Dienste auf **Acronis Managed Machine Service**.
   c. Spezifizieren Sie in der Registerkarte **Anmelden**, bei **Dieses Konto**, den Benutzernamen und das Kennwort, welche Sie verwenden, um sich am Verzeichnisdienst-Wiederherstellungsmodus anzumelden – und klicken Sie dann auf **Aktivieren**.
   d. Klicken Sie in der Registerkarte **Allgemein** auf **Starten**. Klicken Sie nach dem Start des Dienstes auf **OK**.

   Details: Diese Änderung ist notwendig, weil der Acronis Agent Service auf einem Domain-Controller unter einem Domain-Benutzerkonto läuft, Domain-Benutzerkonten sind jedoch im Verzeichnisdienst-Wiederherstellungsmodus (Directory Services Restore Mode, DSRM) nicht verfügbar.
5. Starten Sie Acronis Backup & Recovery 11.5 und stellen Sie die Datenbankdateien aus dem Backup wieder her. Stellen Sie bei Bedarf auch den SYSVOL-Ordner wieder her.

   Details: Weitere Informationen über die Pfade zu diesen Dateien und Ordnern finden Sie unter 'Active Directory-Backup (S. 328). Die Recovery-Prozedur ist ähnlich zu der, die im Abschnitt 'Wiederherstellung von Exchange-Server-Datenbankdateien (S. 332)' beschrieben ist.
6. Sollte die Domain andere Domain-Controller haben, dann stellen Sie sicher, dass kein USN-Rollback-Problem auftritt (S. 338).
7. Starten Sie den Domain-Controller im normalen Modus neu. Stellen Sie sicher, dass der Active Directory-Dienst erfolgreich gestartet wurde.
8. Ändern Sie das Konto für den Acronis-Dienst wieder zurück auf das ursprüngliche, ähnlich wie in Schritt 4.

11.4.4 Wiederherstellung versehentlich gelöschter Informationen

Falls die Domain noch andere Domain-Controller hat, können Sie das Tool **Ntdsutil** verwenden, um eine autorisierte Wiederherstellung nur von bestimmten Einträgen durchführen zu können. Sie können beispielsweise ein unbeabsichtigt gelöschtes Benutzerkonto oder Computerkonto wiederherstellen.

So stellen Sie versehentlich gelöschte Informationen wieder her

1. Führen Sie die Schritte 1 - 5 der Anleitung zur 'Wiederherstellung der Active Directory-Datenbank (S. 336)' aus, um den Domain-Controller im Verzeichnisdienste-Wiederherstellungsmodus (Directory Services Restore Mode, DSRM) neu zu starten und die Active Directory-Datenbank wiederherzustellen.
2. Führen Sie ohne vorhandenen DSRM folgenden Befehl aus:
   ```
   Ntdsutil
   ```


3. Führen Sie in der Eingabeaufforderung des Tools folgende Befehle aus:

```
activate instance ntds
authoritative restore
```

4. Starten Sie in der Eingabeaufforderung des Tools den Befehl **restore subtree** oder **restore object** mit den benötigten Parametern.

   Folgender Befehl stellt beispielsweise das Benutzerkonto **Manager** in der Organisationseinheit **Finance** der Domain **example.com** wieder her:

   ```
   restore object cn=Manager,ou=Finance,dc=example,dc=com
   ```

   Weitere Informationen über die Verwendung des Tools **Ntdsutil** finden Sie in dessen Dokumentation.

   Details: Andere Objekte werden von anderen Domain-Controllern repliziert, wenn Sie den Domain-Controller neu starten. Auf diese Weise stellen Sie die unbeabsichtigt gelöschten Objekte wieder her und behalten Sie die anderen Objekte auf dem neuesten Stand.

5. Starten Sie den Domain-Controller im normalen Modus neu. Stellen Sie sicher, dass der Active Directory-Dienst erfolgreich gestartet wurde – und die wiederhergestellten Objekte verfügbar geworden sind.
6. Ändern Sie das Konto für den Acronis Agent Service wieder zurück auf das ursprüngliche Konto (wie in Schritt 4 des Abschnitts 'Wiederherstellung der Active Directory-Datenbank (S. 336)' beschrieben.

11.4.5 Vermeidung eines USN-Rollbacks

Sollte die Domain über zwei oder mehr Domain-Controller verfügen und sollten Sie einen der Controller oder seine Datenbank wiederherstellen müssen, dann sollten Sie Maßnahmen gegen eine Situation erwägen, die auch als 'USN-Rollback' bekannt ist.

Ein USN-Rollback ist unwahrscheinlich, wenn Sie einen kompletten Domain-Controller von einem VSS-basierten Laufwerk-Backup wiederherstellen.

Ein USN-Rollback ist dagegen deutlich wahrscheinlicher, wenn einer der folgenden Umstände zutrifft:

- Ein Domain-Controller wurde teilweise wiederhergestellt: es wurden nicht alle Laufwerke oder Volumes wiederhergestellt – oder nur die Active Directory-Datenbank.
- Ein Domain-Controller wurde von einem Backup wiederhergestellt, welches ohne VSS erstellt wurde. Das Backup wurde beispielsweise mit einem bootfähigen Medium erstellt. Oder die Option **VSS verwenden** (S. 142) war deaktiviert. Oder der VSS-Provider hatte eine Fehlfunktion.

Die folgenden Informationen helfen Ihnen, ein USN-Rollback mit einigen einfachen Schritten zu vermeiden.

Replikation und USNs

Ein Active Directory wird kontinuierlich zwischen den Domain-Controllern repliziert. Zu jedem Zeitpunkt kann es zu einem Active Directory-Objekt eine neuere Version auf einem Domain-Controller und eine ältere auf einem anderen geben. Um Konflikte und Informationsverluste zu vermeiden, verfolgt das Active Directory Objektversionen auf jedem Domain Controller und ersetzt veraltete Versionen mit aktuellen Versionen.

Um die Objektversionen zu verfolgen, verwendet das Active Directory Zahlen, die Update-Sequenznummern, USNs, Update Sequence Numbers oder Aktualisierungssequenznummern genannt werden. Neuere Versionen von Active Directory-Objekten entsprechen höheren USNs. Jeder Domain Controller bewahrt die USNs von allen anderen Domain Controllern.

USN-Rollback

Nach Durchführung einer nicht autorisierten Wiederherstellung eines Domain Controllers oder seiner Datenbanken wird die aktuelle USN dieses Domain Controllers durch die alte (niedrigere) USN aus dem Backup ersetzt. Die anderen Domain-Controller wissen jedoch nichts von dieser Änderung. Sie haben immer noch die zuletzt bekannte (höhere) USN dieses Domain Controllers beibehalten.

Als Ergebnis treten folgende Probleme auf:

- Der wiederhergestellte Domain Controller verwendet ältere USNs für neue Objekte; er startet mit der alten USN aus dem Backup.
- Die anderen Domain Controller replizieren die neuen Objekte von dem wiederhergestellten Domain-Controller solange nicht, wie dessen USN niedriger bleibt als die USN, von der die anderen Domain-Controller wissen.
- Das Active Directory startet und hat verschiedene Objekte, die zu der gleichen USN korrespondieren, was bedeutet, dass Sie inkonsistent geworden ist. Diese Situation wird USN-Rollback genannt.

Sie müssen zur Vermeidung eines USN-Rollbacks den Domain-Controller über die Tatsache informieren, dass er wiederhergestellt wurde.

So vermeiden Sie ein USN-Rollback

1. Booten Sie direkt nach der Wiederherstellung eines Domain-Controllers oder seiner Datenbanken den wiederhergestellten Domain-Controller und drücken Sie während des Startvorgangs auf F8.
2. Wählen Sie im Fenster **Erweiterte Startoptionen** den Eintrag **Verzeichnisdienst-Wiederherstellungsmodus** – und melden Sie sich dann am Verzeichnisdienste-Wiederherstellungsmodus (DSRM) an.
3. Öffnen Sie den Registry-Editor und erweitern Sie den folgenden Registry-Schlüssel:
   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters
   ```
4. Überprüfen Sie in diesem Registry-Schlüssel den Wert **DSA Previous Restore Count**. Sollte der Wert vorhanden sein, dann notieren Sie sich seine Einstellung. Fügen Sie den Wert nicht hinzu, falls er fehlen sollte.
5. Fügen Sie diesem Registry-Schlüssel folgenden Wert hinzu:
   - Werttyp: **DWORD-Wert (32-Bit)**
   - Wertname: **Von Sicherung wiederhergestellte Datenbank**
   - Datenwert: **1**
6. Starten Sie den Domain-Controller im normalen Modus neu.
7. [Optional] Öffnen Sie nach dem Neustart des Domain Controllers die Ereignisanzeige, erweitern Sie **Anwendungs- und Dienstprotokolle** und wählen Sie das Protokoll **Verzeichnisdienste**. Schauen Sie im Protokoll **Verzeichnisdienste** nach einem kürzlichen Eintrag mit der Ereignis-ID 1109. Sollten Sie diesen Eintrag finden, dann klicken Sie doppelt darauf, um sicherzustellen, dass das Attribut **InvocationID** geändert wurde. Das bedeutet, dass die Active Directory-Datenbank aktualisiert wurde.
8. Öffnen Sie den Registry-Editor und überprüfen Sie, dass die Einstellung im Wert **DSA Previous Restore Count** im Vergleich zu Schritt 4 um den Wert 1 gestiegen ist. Sollte der Wert **DSA Previous Restore Count** in Schritt 4 gefehlt haben, dann überprüfen Sie, dass er nun vorhanden ist und seine Einstellung **1** beträgt.

Sollten Sie eine andere Einstellung sehen (und den Eintrag für die Ereignis-ID 1109 nicht finden können), dann stellen Sie sicher, dass der wiederhergestellte Domain-Controller über die aktuellen Service Packs verfügt und wiederholen Sie dann die komplette Prozedur.

Weitere Details über USNs und USN-Rollback finden Sie in folgendem Microsoft Technet-Artikel: http://technet.microsoft.com/de-de/library/virtual_active_directory_domain_controller_virtualization_hyperv.aspx.

11.5 Wiederherstellung von SharePoint-Daten

Verschiedene SharePoint-Server und SharePoint-Datenbanken werden auf unterschiedliche Art wiederhergestellt.

- Um einzelne Laufwerke oder Volumes eines Front-End-Webservers wiederherzustellen, können Sie entweder mit der grafischen Benutzeroberfläche von Acronis Backup & Recovery 11.5 einen Recovery-Task erstellen (S. 146) – oder den Server mit einem bootfähigen Medium (S. 284) starten und dort die Wiederherstellung konfigurieren.

  Auf gleiche Art können Sie einen SQL Server wiederherstellen.
- Inhaltsdatenbanken können mithilfe des Agenten für SQL (Single-Pass) oder des Agenten für Windows wiederhergestellt werden. Weitere Details finden Sie unter 'Wiederherstellung einer Inhaltsdatenbank (S. 340)'.
- Konfigurations- und Dienstdatenbanken werden als Dateien wiederhergestellt. Weitere Details finden Sie unter 'Wiederherstellung von Konfigurations- und Dienstdatenbanken (S. 342)'.
- Sie können auch einzelne SharePoint-Elemente wiederherstellen (wie Websites, Listen, Dokumentbibliotheken und anderes). Weitere Details finden Sie unter 'Wiederherstellung einzelner Elemente (S. 343)'.

11.5.1 Wiederherstellung einer Inhaltsdatenbank

Dieses Thema beschreibt die Wiederherstellung einer Inhaltsdatenbank zu einer ursprünglichen SharePoint-Farm unter Verwendung von Acronis Backup & Recovery 11.5.

Die Wiederherstellung zu einer 'nicht ursprünglichen' Farm ist eine kompliziertere Prozedur. Diese Schritte variieren in Abhängigkeit von der Farm-Konfiguration und anderen Parametern der Produktionsumgebung.

Eine Inhaltsdatenbank mit dem Agenten für SQL (Single-Pass) wiederherstellen

Diese Methode ermöglicht es Ihnen, eine Datenbank aus dem Single-Pass-Backup einer Maschine wiederherzustellen, auf der der SQL Server läuft.

So stellen Sie eine Inhaltsdatenbank wieder her

1. Verbinden Sie die Konsole mit der Maschine, auf der Sie die Datenbank wiederherstellen wollen. Der Agent für SQL (Single-Pass) muss auf dieser Maschine installiert sein.
2. Stellen Sie die Datenbank gemäß der Beschreibung im Abschnitt 'SQL-Datenbanken zu Instanzen wiederherstellen (S. 351)' zu einer Instanz wieder her.
3. Falls Sie die Datenbank nicht zu dem ursprünglichen SQL Server der ursprünglichen SharePoint-Farm wiederhergestellt haben, dann fügen Sie die wiederhergestellte Datenbank an die Farm an. Führen Sie dazu folgenden Befehl auf einem Front-End-Webserver aus:

   In SharePoint 2010 oder höher:
   ```
   Mount-SPContentDatabase <Datenbank> -DatabaseServer <Datenbankserver>
   -WebApplication <Site-URL>
   ```

Bei SharePoint 2007:

```
stsadm.exe -o addcontentdb -url <Site-URL> -databasename <Datenbank>
-databaseserver <Datenbankserver>
```

Eine Inhaltsdatenbank mit dem Agenten für Windows wiederherstellen

Diese Methode ermöglicht es Ihnen, eine Datenbank aus dem Laufwerk-Backup einer Maschine wiederherzustellen, auf der der SQL Server läuft.

So stellen Sie eine Inhaltsdatenbank zu dem ursprünglichen SQL Server wieder her

1. Falls der Dienst 'Windows SharePoint Services Timer' läuft, stoppen Sie den Dienst und warten Sie einige Minuten, damit irgendwelche laufenden gespeicherten Prozeduren abgeschlossen werden können. Starten Sie den Dienst nicht neu, bis Sie alle Datenbanken, die wiederhergestellt werden müssen, auch wiederhergestellt haben.
2. Falls Sie die Datenbank zu dem ursprünglichen Speicherplatz auf dem Laufwerk wiederherstellen, dann tun Sie Folgendes:
   a. Bringen Sie die Zieldatenbank offline.
   b. Stellen Sie die Datenbankdateien so wie unter 'Wiederherstellung von SQL Server-Datenbanken von einem Laufwerk-Backup (S. 330)' beschrieben wieder her, mit Ausnahme des Schritts zum Anfügen der Datenbank (die Datenbank ist bereits angefügt).
   c. Bringen Sie die wiederhergestellte Datenbank online.

   Falls Sie die Datenbank zu einem anderen Speicherort auf dem Laufwerk wiederherstellen, dann stellen Sie die Datenbankdateien wie unter 'Wiederherstellung von SQL Server-Datenbanken von einem Laufwerk-Backup (S. 330)' beschrieben wieder her, einschließlich des Schrittes zum Anfügen der Datenbank.
3. Starten Sie den Windows SharePoint Services Timer-Dienst.

So stellen Sie eine Inhaltsdatenbank zu einem anderen SQL auf der ursprünglichen Farm wieder her

1. Entfernen Sie von der SharePoint-Farm diejenige Datenbank, die Sie später wiederherstellen werden. Führen Sie dazu folgenden Befehl auf einem Front-End-Webserver aus:

   In SharePoint 2010 oder höher:

   ```
   Dismount-SPContentDatabase <Datenbank>
   ```

   Falls Sie mehrere Inhaltsdatenbanken mit demselben Namen haben, müssen Sie statt des Namens die GUID der Inhaltsdatenbank in diesem Befehl verwenden. Um die GUID der Inhaltsdatenbank abfragen zu können, müssen Sie die das Cmdlet ***`Get-SPContentDatabase`*** *ohne Argumente ausführen.*

   Bei SharePoint 2007:

   ```
   stsadm -url <Webapplikations-URL> –o deletecontentdb –databasename <Datenbank>
   ```
2. Stellen Sie die Datenbankdateien so wie unter 'Wiederherstellung von SQL Server-Datenbanken von einem Laufwerk-Backup (S. 330)' beschrieben wieder her, einschließlich des Schrittes zum Anfügen der Datenbank.
3. Fügen Sie die wiederhergestellte Datenbank an die SharePoint-Farm an. Führen Sie dazu folgenden Befehl auf einem Front-End-Webserver aus:

   In SharePoint 2010 oder höher:

   ```
   Mount-SPContentDatabase <Datenbank> -DatabaseServer <Datenbankserver>
   -WebApplication <Site-URL>
   ```

   Bei SharePoint 2007:

   ```
   stsadm.exe -o addcontentdb -url <Site-URL> -databasename <Datenbank>
   -databaseserver <Datenbankserver>
   ```

11.5.2 Wiederherstellung von Konfigurations- und Dienstdatenbanken

Konfigurations- und Dienstdatenbanken müssen mit anderen Datenbanken synchronisiert werden. Es ist daher empfehlenswert, Konfigurations- und Dienstdatenbanken entweder zusammen mit Inhaltsdatenbanken wiederherzustellen – oder zu ihrem letzten Zeitpunkt (falls die Inhaltsdatenbanken keine Wiederherstellung benötigen).

Die Konfigurationsdatenbank enthält Host-Namen der Farm-Server. Daher können Sie die Konfigurationsdatenbank nur zu der ursprünglichen SharePoint-Farm wiederherstellen. Dienstdatenbanken können zu einer nicht ursprünglichen Farm wiederhergestellt werden.

So stellen Sie die Konfigurationsdatenbank wieder her

1. Stoppen Sie auf dem Server, der die Website **Zentraladministration** ausführt, im Snap-in **Dienste** die in der unteren Tabelle aufgelisteten Dienste.
2. Führen Sie folgenden Befehl auf dem Server aus, der die Site **Zentraladministration** ausführt:
```
iisreset /stop
```
3. Stellen Sie die Datenbankdateien so wie unter 'Wiederherstellung von SQL Server-Datenbanken von einem Laufwerk-Backup (S. 330)' beschrieben wieder her.
4. Starten Sie die SharePoint-Dienste wieder, die zuvor gestoppt wurden.

SharePoint 2007-Dienste	SharePoint 2010-Dienste	SharePoint 2013-Dienste
▪ **Microsoft Dienst für einmaliges Anmelden** ▪ **Office-Startprogrammdienst für die Dokumentkonvertierung** ▪ **Office-Lastenausgleichsmodul-Dienst für die Dokumentkonvertierung** ▪ **Office SharePoint Server-Suchdienst** ▪ **Windows SharePoint Services-Verwaltung** ▪ **Windows SharePoint Services-Suche** ▪ **Windows SharePoint Services-Timer** ▪ **Windows SharePoint Services-Ablaufverfolgung** ▪ **Windows SharePoint Services VSS Writer**	▪ **SharePoint 2010-Verwaltungsdienst** ▪ **SharePoint 2010 Timerdienst** ▪ **SharePoint 2010-Ablaufverfolgungsdienst** ▪ **SharePoint 2010 User Code Host** ▪ **SharePoint 2010 VSS Writer** ▪ **WWW-Publishingdienst** ▪ **SharePoint Server Search 14** ▪ **SharePoint Foundation Search V4** ▪ **Web Analytics-Datenverarbeitungsdienst** ▪ **Web Analytics-Webdienst**	▪ **SharePoint-Administration** ▪ **SharePoint-Timer** ▪ **SharePoint-Ablaufverfolgung** ▪ **SharePoint User Code Host** ▪ **SharePoint VSS Writer** ▪ **WWW-Publishingdienst** ▪ **SharePoint Server-Suche**

So stellen Sie eine Dienstdatenbank wieder her

1. Stoppen Sie die Dienste, die mit den wiederherzustellenden Datenbanken assoziiert sind. Gehen Sie folgendermaßen vor:
   a. Öffnen Sie die Seite **Zentraladministration**.
   b. Wählen Sie eine der nachfolgenden Varianten:

Wählen Sie in SharePoint 2010 (oder höher) **Systemeinstellungen** –> **Dienste auf dem Server verwalten**.

Wählen Sie in SharePoint 2007 **Vorgänge** –> **Dienste auf dem Server**.

c. Klicken Sie zum Ändern des Servers, auf dem Sie den Dienst stoppen wollen, in der Liste **Server** auf **Server ändern** und klicken Sie dann auf den gewünschten Server-Namen.

d. Standardmäßig werden nur konfigurierbare Dienste angezeigt. Klicken Sie in der Liste **Ansicht** auf **Alle**, um alle Dienste anzuzeigen.

e. Klicken Sie auf **Beenden** in der Spalte **Aktion** des entsprechenden Dienstes, um einen Dienst zu stoppen.

f. Klicken Sie auf **OK**, um den Dienst zu stoppen.

2. Stellen Sie die Datenbankdateien so wie unter 'Wiederherstellung von SQL Server-Datenbanken von einem Laufwerk-Backup (S. 330)' beschrieben wieder her.
3. Starten Sie, ähnlich wie in Schritt 1, die mit den Datenbanken assoziierten Dienste.

11.5.3 Wiederherstellung einzelner Elemente

Verwenden Sie eine der folgenden dreit Methoden zur Wiederherstellung einzelner SharePoint-Elemente:

- Acronis SharePoint Explorer verwenden. Dieses Tool ermöglicht es Ihnen, SharePoint-Elemente von Single-Pass-Laufwerk- und Anwendungs-Backups (S. 345), von einer angebundenen Datenbank oder von Datenbankdateien wiederherzustellen.

  Um das Tool verwenden zu können, müssen Sie eine funktionierende SharePoint-Farm haben. Sie müssen außerdem eine Lizenz für das Acronis Backup & Recovery 11.5 Microsoft SharePoint Add-on erwerben.

  Sie können auf Acronis SharePoint Explorer zugreifen, indem Sie im Menü **Extras** der Acronis Backup & Recovery 11.5 Management Console auf den Befehl **SharePoint-Daten extrahieren** klicken. Weitere Informationen über das Tool finden Sie in dessen Dokumentation: http://www.acronis.de/support/documentation/ASPE/.
- Anfügen der Inhaltsdatenbank an eine 'nicht ursprüngliche' SharePoint-Farm (beispielsweise eine SharePoint-Wiederherstellungsfarm).

  Es ist notwendig, die Inhaltsdatenbank an eine nicht ursprüngliche SharePoint-Farm anzufügen, weil jedes Objekt in einer Farm eine eindeutige ID haben muss. Sie können daher die Datenbank nicht an die ursprüngliche Farm anfügen.
- Wiederherstellung von einer nicht angefügten Datenbank Diese Methode ist für SharePoint 2007 nicht verfügbar.

  Diese Methode ermöglicht es Ihnen nur, die folgenden Elementtypen wiederherzustellen: Websites, Listen oder Dokumentbibliotheken.

So stellen Sie SharePoint-Elemente durch Anfügen der Inhaltsdatenbank zu einer Farm wieder her

1. Fügen Sie die Inhaltsdatenbank einer SQL Server-Instanz an, wie es in den Schritten 1-5 der Anleitung 'Zugriff auf SQL Server-Datenbanken von einem Laufwerk-Backup aus (S. 331)' beschrieben ist.
2. Fügen Sie die Inhaltsdatenbank einer nicht ursprünglichen SharePoint-Farm an. Gehen Sie folgendermaßen vor:

   a. Stellen Sie sicher, dass Sie diese Prozedur unter einem Farm-Administratorkonto durchführen, welches ein Mitglied der Rolle **db_owner** der Datenbank ist. Ist das nicht der

Fall, dann verwenden Sie Microsoft SQL Server Management Studio, um das Konto dieser Rolle hinzuzufügen.

b. Führen Sie folgenden Befehl auf einem Front-End-Webserver aus:

   In SharePoint 2010 oder höher:

```
Mount-SPContentDatabase <Datenbank> -DatabaseServer <Datenbankserver>
-WebApplication <Website-URL>
```

   Bei SharePoint 2007:

```
stsadm.exe -o addcontentdb -url <Website-URL> -databasename <Datenbank>
-databaseserver <Datenbankserver>
```

3. Öffnen Sie die SharePoint-Website und wählen Sie das herunterzuladende Dokument.
4. Trennen Sie die Inhaltsdatenbank nach dem Abschluss des Downloads wieder von der SharePoint-Farm.
5. Trennen Sie die Datenbank und dann das zuvor gemountete Volume, wie in den Schritten 7-8 der Anleitung 'Zugriff auf SQL Server-Datenbanken von einem Laufwerk-Backup aus (S. 331)' beschrieben.

So stellen Sie SharePoint-Elemente von einer nicht angefügten Datenbank wieder her

1. Fügen Sie die Inhaltsdatenbank einer SQL Server-Instanz an, wie es in den Schritten 1-5 der Anleitung 'Zugriff auf SQL Server-Datenbanken von einem Laufwerk-Backup aus (S. 331)' beschrieben ist.
2. Stellen Sie die Daten gemäß der Beschreibung unter 'http://technet.microsoft.com/de-de/library/hh269602' wieder her.
3. Trennen Sie die Datenbank und dann das zuvor gemountete Volume, wie in den Schritten 7-8 der Anleitung 'Zugriff auf SQL Server-Datenbanken von einem Laufwerk-Backup aus (S. 331)' beschrieben.

12 Microsoft SQL Server mit Single-Pass-Backups schützen

Dieser Abschnitt beschreibt, wie Sie Single-Pass-Laufwerk- und Anwendungs-Backups verwenden, um Microsoft SQL Server-Daten zu schützen.

Eine Single-Pass-Backup-Aktion erstellt ein anwendungssensitives Laufwerk-Backup, welches Ihnen ermöglicht, die so gesicherten Anwendungsdaten zu durchsuchen und wiederherzustellen, ohne das komplette Laufwerk oder Volume wiederherstellen zu müssen. Das Laufwerk oder Volume kann außerdem auch als Ganzes wiederhergestellt werden. Das bedeutet, dass eine einzelne Lösung und ein einzelner Backup-Plan gleichermaßen für Desaster-Recovery als auch zum Schutz der Daten verwendet werden kann. Die Anwendungsprotokolle können bei Bedarf nach dem Backup abgeschnitten werden.

Die Single-Pass-Backup-Funktionalität steht Ihnen zur Verfügung, wenn Sie den Acronis Backup & Recovery 11.5 Agenten für Microsoft SQL Server (Single-Pass) installieren.

Ohne diesen Agenten können Sie Ihre SQL Server-Daten mithilfe von Backups auf Laufwerkebene schützen. Eine detaillierte Beschreibung dieser Methode finden Sie im Abschnitt 'Anwendungen mit Laufwerk-Backups schьtzen (S. 318)'.

Microsoft SharePoint schützen

Eine Microsoft SharePoint-Farm besteht aus Front-End-Webservern und Maschinen mit Microsoft SQL Servern. Das bedeutet, dass die in diesem Abschnitt präsentierten Informationen auch für den Schutz von Microsoft SharePoint-Daten gelten.

Empfehlungen zum speziellen Backup von Maschinen mit SharePoint-Daten finden Sie im Abschnitt 'SharePoint-Daten-Backup (S. 329)'.

Informationen über die Wiederherstellung von SharePoint-Daten finden Sie im Abschnitt 'Wiederherstellung von SharePoint-Daten (S. 340)'.

12.1 Allgemeine Informationen

12.1.1 Agent für SQL (Single-Pass)

Single-Pass-Backups (Einzeldurchlauf-Backups) von Microsoft SQL Server-Daten stehen Ihnen zur Verfügung, wenn Sie den Acronis Backup & Recovery 11.5 Agenten für Microsoft SQL Server (Single-Pass) verwenden. Der Agent wird in diesem Dokument auch als Agent für SQL (Single-Pass) bezeichnet.

Backup

Während eines Laufwerk-Backups fügt der Agent für SQL (Single-Pass) der resultierenden Backup-Datei bestimmte Metadaten vom Microsoft SQL Server hinzu. Durch Verwendung dieser Metadaten erkennt und katalogisiert Acronis Backup & Recovery 11.5 die SQL Server-Datenbanken. Nachdem das Backup erfolgreich abgeschlossen wurde, beschneidet der Agent das SQL Server-Transaktionsprotokoll, sofern die entsprechende Option im Backup-Plan eingestellt wurde.

Recovery

Der Agent ermöglicht Ihnen, SQL-Datenbanken direkt zu einer laufenden SQL Server-Instanz wiederherzustellen. Sie können eine Datenbank sofort für Benutzer verfügbar machen oder erst weitere Aktionen durchführen, bevor Sie sie dann verfügbar machen.

Der Agent kann außerdem Datenbankdateien von einem Single-Pass-Backup zu einem Ordner im Dateisystem extrahieren. Diese Dateien können zur Datengewinnung oder für Überprüfungszwecke verwendet werden. Bei einem Notfall können Sie diese Datenbankdateien an eine SQL Server-Instanz anschließen, die nicht von einem Agenten verwaltet wird.

Datenbanken mounten

Sie können mithilfe des Agenten eine in einem Backup gesicherte Datenbank an eine laufende SQL Server-Instanz anschließen und dann Dritthersteller-Tools verwenden, um unterschiedliche Objekte aus der Datenbank abzurufen.

12.1.2 Unterstützte Betriebssysteme

Der Agent für SQL (Single-Pass) kann auf folgenden Betriebssystemen installiert werden:

Windows Server 2003/2003 R2 – Standard und Enterprise Editionen (x86, x64)
Windows Small Business Server 2003/2003 R2
Windows Server 2008 – Standard, Enterprise und Datacenter Editionen (x86, x64)
Windows Small Business Server 2008
Windows 7 – alle Editionen mit Ausnahme der Starter und Home Editionen (x86, x64)
Windows Server 2008 R2 – Standard, Enterprise, Datacenter und Foundation Editionen
Windows MultiPoint Server 2010/2011
Windows Small Business Server 2011 – alle Editionen
Windows 8/8.1 – alle Editionen mit Ausnahme der Windows RT-Editionen (x86, x64)
Windows Server 2012/2012 R2 – alle Editionen
Windows Storage Server 2003/2008/2008 R2/2012

12.1.3 Unterstützte Microsoft SQL Server-Versionen

Der Agent for SQL (Single-Pass) unterstützt folgende Microsoft SQL Server-Versionen:

- Microsoft SQL Server 2005
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012

12.1.4 Berechtigungen für SQL Server-Backup und -Recovery

Für ein Single-Pass-Backup erforderliche Berechtigungen

Um von einer Maschine, auf der ein Microsoft SQL Server läuft, erfolgreich ein Single-Pass-Backup erstellen zu können, muss das unter dem Backup-Plan laufende Konto auf der Maschine ein Mitglied der Gruppe **Sicherungs-Operatoren** oder **Administratoren** sein.

Diesem Konto muss außerdem die **SysAdmin**-Rolle für alle auf der Maschine installierte Instanzen zugewiesen sein.

Sollten Sie einen Backup-Plan erstellen, während Sie als normaler Benutzer (etwa als Mitglied der Gruppe **Benutzer**) angemeldet sind, dann müssen Sie die Anmeldedaten für ein Konto spezifizieren, das über die oberen Berechtigungen verfügt. Klicken Sie, um auf diese Einstellung zugreifen zu können, in der Seite **Backup-Plan erstellen** (S. 58) auf **Anmeldedaten des Plans**.

Ein Backup-Plan, der von einem Mitglied der Gruppe **Administratoren** erstellt wird, läuft standardmäßig unter dem Konto des Agenten-Dienstes (Agent Service). Dasselbe gilt auch für einen zentralen Backup-Plan, der vom Management Server aus bereitgestellt wurde. Das ist der Grund, warum es ratsam ist, dem Agenten die für Single-Pass-Backups erforderlichen Berechtigungen zuzuweisen.

Dem Agenten Berechtigungen erteilen

Das Setup-Programm bindet während der Installation das Konto des Agenten-Dienstes in die Gruppe der **Sicherungs-Operatoren** ein. Falls Sie sich dazu entschließen, ein neues Konto für den Agenten zu erstellen, dann wird dieses Konto außerdem in die Gruppe der **Administratoren** aufgenommen. Der Agent hat daher unter Windows immer die erforderlichen Berechtigungen.

Um dem Agenten die **SysAdmin**-Rolle im SQL Server zuweisen zu können, werden Sie aufgefordert, die **SysAdmin**-Anmeldedaten für jede auf der Maschine installierte Microsoft SQL-Instanz zu spezifizieren. Wenn Sie während der Installation keine Anmeldedaten spezifizieren, können Sie dem Agenten die **SysAdmin**-Rolle auch später zuweisen – und zwar mit einer der folgenden Varianten:

- Indem Sie auf **Extras** –> **SQL Server-Anmeldedaten bereitstellen** klicken, wenn die Acronis Backup & Recovery 11.5 Management Console mit der Maschine verbunden ist.
- Durch Verwendung von Microsoft SQL Server Management Studio.
- Durch Ausführung eines T-SQL-Skripts.

Sie müssen dem Agenten zudem ausdrücklich die **SysAdmin**-Rolle gewähren, nachdem eine neue Microsoft SQL Server-Instanz auf der Maschine installiert wurde.

So weisen Sie dem Konto des Agenten-Dienstes die** SysAdmin**-Rolle für eine Instanz mithilfe eine T-SQL-Skript zu

1. Erstellen Sie eine Textdatei mit folgendem Inhalt:

```
Create Login [<Maschinenname>\Acronis Agent User] From Windows
Exec master..sp_addsrvrolemember @loginame = '<Maschinenname>\Acronis Agent
User',@rolename = 'sysadmin'
```

   Acronis Agent User ist das für den Agenten standardmäßig erstellte Konto. Sollten Sie während der Agenten-Installation ein bereits vorhandenes Konto spezifiziert haben, dann ersetzen Sie **Acronis Agent User** mit dem Benutzernamen dieses vorhandenen Kontos.

   Die Datei kann jede beliebige Erweiterung haben.

2. Führen Sie in der Eingabeaufforderung folgenden Befehl aus:

```
sqlcmd -S <Maschinenname>\<Instanzname> -i <vollständiger Pfad zur
T-SQL-Skriptdatei>
```

Falls Sie dem Agenten die **SysAdmin**-Rolle nicht zuweisen wollen, dann müssen Sie die Anmeldedaten in jedem Backup-Plan spezifizieren (wie am Anfang dieses Abschnitts beschrieben).

Zur Wiederherstellung einer Microsoft SQL Server-Datenbank erforderliche Berechtigungen

Wenn Sie eine Datenbank zu einer Instanz wiederherstellen, müssen Sie die Anmeldedaten für diese Instanz spezifizieren. Die Eingabeaufforderung für die Anmeldedaten erscheint, nachdem Sie die Zielinstanz auf der Seite '**Daten wiederherstellen** (S. 146)' ausgewählt haben.

12.1.5 Was Sie sonst noch über Single-Pass-Backups wissen sollten

Ein Single-Pass-Backup (Einzeldurchlauf-Backup) wird auf Laufwerksebene durchgeführt. Das bedingt folgende Besonderheiten für diesen Backup-Typ:

- Auf Netzwerkfreigaben liegende Datenbanken können nicht gesichert werden.
- Dateigruppen werden als komplette Datenbank gesichert und wiederhergestellt. Eine einzelne Datei kann nicht wiederhergestellt werden, so dass die Datenbank betriebsbereit ist.
- Datenbank können nicht zu einem beliebigen Zeitpunkt wiederhergestellt werden, sondern nur zu Zeitpunkten, an denen ein Daten-Snapshot erfasst wurde. Falls Sie Backups der Transaktionsprotokolle unter Verwendung der 'Sichern und Wiederherstellen'-Komponente des SQL Servers erstellen, können Sie zusätzlich diese Protokolle anwenden, um einen gewünschten Recovery-Punkt zu erreichen.

12.2 Installation des Agenten für SQL (Single-Pass)

Der Agent für SQL (Single-Pass) kann nur auf einer Maschine installiert werden, auf der der Microsoft SQL Server läuft. Eine Remote-Installation des Agenten ist nicht möglich.

Der Agent ist in den Setup-Programmen der Standalone- und Advanced-Editionen von Acronis Backup & Recovery 11.5 enthalten. Die vom Agenten bereitgestellte Funktionalität ist in beiden Setup-Programmen gleich.

Der Agent für SQL (Single-Pass) wird als Add-on des Agenten für Windows installiert.

Erforderliche Lizenzen

Verwenden Sie zur Installation des Agenten für Windows eine beliebige Lizenz, die es ermöglicht, den Agenten zu installieren.

Falls der Agenten für Windows mit einer Advanced Server SBS Edition-Lizenz installiert wird, können Sie den Agenten für SQL (Single-Pass) ohne eine zusätzliche Lizenz installieren. Verwenden Sie anderenfalls eine der folgenden Lizenzen:

- Acronis Backup & Recovery 11.5 Microsoft SQL Server Add-on
- Acronis Backup & Recovery 11.5 Microsoft SharePoint Add-on

Jede dieser Lizenzen ermöglicht Ihnen die Installation des Agenten für SQL (Single-Pass) auf einem physikalischen Host und auf vier virtuellen Maschinen, die auf demselben Host laufen. Beachten Sie, dass zusammen mit dem Agenten für SQL (Single-Pass) auf jeder virtuellen Maschine auch der Agent für Windows installiert werden muss.

Zur Verwendung des Produktes im Testmodus benötigen Sie keine Lizenzen.

Installation

Installieren Sie den Agenten auf gleiche Weise wie den Agenten für Windows. Detaillierte Schritt-für-Schritt-Anweisungen finden Sie in folgenden Abschnitten der Installationsanleitung:

- 'Interaktive Installation in den Standalone-Editionen'.
- 'Interaktive Installation in den Advanced-Editionen'.

Anmeldedaten für Microsoft SQL-Instanzen

Sie werden während der Installation aufgefordert, **SysAdmin**-Anmeldedaten für jede auf der Maschine installierte Microsoft SQL-Instanz zu spezifizieren. Diese Anmeldedaten werden benötigt, um dem Konto des Agenten-Dienstes die **SysAdmin**-Rolle zu gewähren.

Sie können die Eingabe der Anmeldedaten überspringen und dem Agenten die **SysAdmin**-Rolle auch auf eine der folgenden Arten später zuweisen:

- Indem Sie auf **Extras** –> **SQL Server-Anmeldedaten bereitstellen** klicken, wenn die Acronis Backup & Recovery 11.5 Management Console mit der Maschine verbunden ist.
- Durch Verwendung von Microsoft SQL Server Management Studio.
- Durch Ausführung eines T-SQL-Skripts.

Zu weiteren Informationen siehe den Abschnitt 'Berechtigungen fьr SQL Server-Backup und -Recovery (S. 346)' in der Produkthilfe oder der Benutzeranleitung.

12.3 Microsoft SQL Server per Backup sichern

Um einen Microsoft SQL Server schützen zu können, können Sie einen Backup-Plan erstellen oder die Funktion **Backup jetzt** verwenden (wie im Abschnitt 'Backup (S. 58) beschrieben).

Folgen Sie diesen Anweisungen, um sicherzustellen, dass ein Single-Pass-Backup erfolgreich ist.

- **Backup kompletter Maschinen. Dies ermöglicht Ihnen, sowohl das Betriebssystem als auch jede auf der Maschine vorhandene SQL-Datenbank wiederherzustellen.**

  Datenbanken können auf mehr als einem Laufwerk oder Volume gespeichert sein. Um sicherzustellen, dass alle benötigten Dateien in einem Backup enthalten sind, sollten Sie die komplette Maschine sichern. Das gewährleistet außerdem, dass der SQL Server weiterhin geschützt bleibt, wenn Sie noch mehr Datenbanken hinzufügen oder zukünftig die Protokolldateien verlagern.
- **Sollten Sie nicht die komplette Maschine sichern wollen, dann wählen Sie die Volumes sorgfältig aus.**

  Sollten Sie sicher sein, dass die Datenbanken und damit assoziierte Dateien immer auf denselben Volumes vorliegen, dann möchten Sie möglicherweise nur Backups dieser Volumes erstellen. Oder Sie möchten separate Backup-Pläne für das System-Volume und diejenigen Volumes erstellen, welche die Daten speichern.

  Sie können außerdem Dateien und Ordner ausschlieЯen (S. 63), falls Sie sicher sind, dass Sie nicht zum Microsoft SQL Server gehören.

  Stellen Sie in jedem Fall sicher, dass alle Volumes, die notwendige Dateien enthalten, in das Backup aufgenommen werden. Sollte beispielsweise die Protokolldatei einer Datenbank nicht in das Backup aufgenommen werden, dann können Sie diese Datenbank später nicht mehr wiederherstellen. Die Wiederherstellung eines Betriebssystems ist wahrscheinlich nicht mehr möglich, wenn Sie das Boot- oder System-Volume nicht mitgesichert oder kritische Systemdateien ausgeschlossen haben.

  Anweisungen darüber, wie Sie die Datenbankpfade ermitteln können, finden Sie im Abschnitt 'SQL Server-Datenbankdateien (S. 320)'.
- **Volumen-Schattenkopie (VSS) verwenden.**

Stellen Sie sicher, dass die Backup-Option Volume Shadow Copy Service (S. 142) auf **Volume Shadow Copy Service verwenden** eingestellt ist und dass der ausgewählte Snapshot-Provider nicht auf **Software – Acronis VSS Provider** steht. Die beste Wahl ist **Software – System-Provider**.

12.3.1 Einstellungen für Single-Pass-Backup

Die in diesem Abschnitt beschriebenen Einstellungen gelten für Single-Pass-Backups (Einzeldurchlauf-Backups). Diese Einstellungen sind im Abschnitt **Single-Pass-Laufwerk- und Anwendungs-Backup** der Seiten **Backup-Plan erstellen** (S. 58) oder **Backup jetzt** (S. 58) in eine Gruppe zusammengefasst.

Single-Pass-Backup

Diese Einstellung aktiviert Single-Pass-Laufwerk- und Anwendungs-Backups.

Um auf die folgenden Einstellungen zugreifen zu können, klicken Sie auf **Task-Fehlerbehandlung, Protokollabschneidung anzeigen**.

Fehlerbehandlung

Das Kontrollkästchen **Anwendungs-Backup-Fehler ignorieren und den Task fortsetzen** bestimmt das Verhalten der Software, wenn das Sammeln von Anwendungsmetadaten während eines Backups fehlschlägt. Dies passiert beispielsweise, falls eine Datenbank beschädigt ist, der Anwendungsdienst gestoppt ist, die VSS-Verwendung in den Backup-Optionen deaktiviert ist oder dem Konto, unter dem das Backup läuft, die Berechtigungen zum Zugriff auf eine Datenbank fehlen.

Standardmäßig lässt Acronis Backup & Recovery 11.5 das Backup fehlschlagen.

Falls Sie das Kontrollkästchen aktivieren, wird das Backup fortgesetzt. Das Ereignisprotokoll wird einen Eintrag für jede Datenbank enthalten, für die keine Metadaten gesammelt wurden. Falls überhaupt keine Metadaten gesammelt werden, dann erhalten Sie ein gewöhnliches Laufwerk-Backup.

Die folgende Einstellung ist nur dann verfügbar, wenn der Agent für SQL (Single-Pass) auf der Maschine installiert ist.

Protokollabschneidung

Ist diese Einstellung aktiviert, dann wird das Microsoft SQL Server-Protokoll nach jedem vollständigen, inkrementellen oder differentiellen Backup abgeschnitten. Das Abschneiden erfolgt nur, wenn das Single-Pass-Backup (Einzeldurchlauf-Backup) erfolgreich war.

Lassen Sie die Einstellung deaktiviert, falls Sie zur Sicherung der SQL Server-Daten eine Dritthersteller-Anwendung verwenden (wie beispielsweise die 'Sichern und Wiederherstellen'-Komponente des SQL Servers).

Protokollabschneidung und das Ignorieren von Anwendungsfehlern schließen sich gegenseitig aus. Das verhindert ein Abschneiden des Microsoft SQL-Protokolls, falls keine Awendungsmetadaten gesammelt werden.

12.4 Wiederherstellung von Microsoft SQL Server-Daten

Dieser Abschnitt beschreibt nur die Schritte und Einstellungen, die zur Wiederherstellung von SQL-Datenbanken von einem Single-Pass-Backup (Einzeldurchlauf-Backup) spezifisch sind. Die allgemeinen Einstellungen eines Recovery-Tasks sind im Abschnitt 'Einen Recovery-Task erstellen (S. 146)' beschrieben.

Sie haben zwei Optionen für eine SQL-Datenbank-Wiederherstellung:

- **Datenbanken zu Instanzen wiederherstellen (S. 351).**

- **Datenbankdateien zu Ordnern extrahieren (S. 353).**

12.4.1 SQL-Datenbanken zu Instanzen wiederherstellen

Sie können innerhalb eines einzelnen Recovery-Tasks mehrere Datenbanken wiederherstellen. Die Datenbanken werden ihren ursprünglichen Instanzen automatisch zugeordnet. Sie können bei Bedarf für jede Datenbank eine Zielinstanz wählen.

Systemdatenbanken werden auf gleiche Weise wie Benutzerdatenbanken wiederhergestellt. Bei Wiederherstellung der **Master**-Datenbank startet die Software die Zielinstanz automatisch im Einzelbenutzermodus neu. Nach Abschluss der Wiederherstellung startet die Software die Instanz neu und und stellt andere Datenbanken (sofern vorhanden) wieder her. Weitere, bei Wiederherstellung einer Systemdatenbank zu beachtende Punkte:

- Eine Systemdatenbank kann nur zu einer Instanz mit derselben Version wie die ursprüngliche Instanz wiederhergestellt werden.
- Eine Systemdatenbank kann nur im Stadium 'Verwendungsbereit' (ready to use) wiederhergestellt werden.
- Weil die **Master**-Datenbank Informationen über alle Datenbanken der Instanz aufnimmt, müssen Sie evtl. nach Wiederherstellung der Datenbank weitere Aktionen durchführen. Weitere Details finden Sie unter 'Aktionen nach Wiederherstellung einer Masterdatenbank (S. 352)'.

So stellen Sie Datenbanken zu einer Instanz wieder her

Auf der Seite **Daten wiederherstellen**:

1. Klicken Sie unter **Recovery-Quelle** auf **Daten wählen** und bestimmen Sie die entsprechenden Datenbanken.
2. Falls die Konsole mit dem Management Server verbunden ist, dann wählen Sie diejenige registrierte Maschine aus, wo die Datenbanken wiederhergestellt werden sollen. Ansonsten können Sie diesen Schritt überspringen.
3. Wählen Sie **Datenbanken zu Instanzen wiederherstellen**.
4. Acronis Backup & Recovery 11.5 versucht die Zielinstanzen für die gewählten Datenbanken zu spezifizieren, indem es die ursprünglichen Pfade aus dem Backup nimmt. Falls die Zielinstanz für keine Datenbank ausgewählt ist oder falls Sie die Datenbank zu einer anderen Instanz wiederherstellen wollen, dann spezifizieren Sie die Zielinstanz manuell.

   Sollten die Berechtigungen Ihres aktuellen Kontos nicht ausreichen, um auf die SQL Server-Zielinstanz zuzugreifen, dann werden Sie nach den Anmeldedaten gefragt.
5. Sollte die Zielinstanz eine Datenbank enthalten, die den gleichen Namen wie die wiederherzustellende hat, dann zeigt die Software eine Warnmeldung an: **Die Zieldatenbank existiert bereits.**. Sie haben folgende Optionen:
   - **Existierende Datenbanken überschreiben**

     Dies ist die für die meisten Situationen passende Standardeinstellung. Die Datenbank in der Zielinstanz wird durch die Datenbank aus dem Backup überschrieben.
   - **Die wiederhergestellte Datenbank umbenennen**

     Diese Einstellung ermöglicht Ihnen, die vorhandene Datenbank zu behalten. Eine wiederhergestellte Datenbank erhält folgenden Namen: <ursprünglicher Datenbankname>**-Recovered**. Sollte eine Datenbank mit diesem Namen bereits existieren, dann wird die wiederhergestellte Datenbank folgendermaßen benannt: <ursprünglicher Datenbankname>**-Recovered (**<fortlaufende Nummer>**)**.

     Beispiele: **MyDatabase-Recovered**, **MyDatabase-Recovered (2)**.

6. Sie können für jede wiederherzustellende Datenbank ihr Stadium nach der Wiederherstellung bestimmen. Klicken Sie dazu links neben dem Datenbanknamen auf das Symbol ▷ und wählen Sie dann einen der folgenden Werte:
   - **Verwendungsbereit (Mit RECOVERY wiederherstellen)** (Standardeinstellung)

     Die Datenbank ist nach Abschluss der Wiederherstellung direkt einsatzbereit. Benutzer haben vollen Zugriff auf sie. Die Software wird für alle Transaktionen der wiederhergestellten Datenbank ein Rollback ausführen, für die kein 'Commit' ausgeführt wurde und die in den Transaktionsprotokollen gespeichert sind. Sie können keine zusätzlichen Transaktionsprotokolle von systemeigenen Microsoft SQL-Backups wiederherstellen.
   - **Nicht betriebsbereit (Mit NORECOVERY wiederherstellen)**

     Die Datenbank ist nach Abschluss der Wiederherstellung nicht betriebsbereit. Benutzer haben keinen Zugriff auf sie. Die Software behält alle nicht übernommenen Transaktionen (ohne 'Commit') der wiederhergestellten Datenbank. Sie können zusätzliche Transaktionsprotokolle von systemeigenen Microsoft SQL-Backups wiederherstellen und auf diese Weise den notwendigen Recovery-Punkt erreichen.
   - **Schreibgeschützt (Mit STANDBY wiederherstellen)**

     Benutzer haben nach Abschluss der Wiederherstellung einen 'Nur Lesen'-Zugriff auf die Datenbank. Die Software wird alle nicht übernommenen Transaktionen (ohne 'Commit') rückgängig machen. Die Rückgängigaktionen werden jedoch in einer temporären Standby-Datei gespeichert, so dass die Recovery-Effekte zurückgestellt werden werden können.

     Dieser Wert wird primär verwendet, um den Zeitpunkt eines SQL Server-Fehlers zu ermitteln.
7. Sie können die Pfade auf die Orte ändern, wo die Datenbankdateien gespeichert werden. Klicken Sie links neben dem Datenbanknamen auf das Symbol ▷, um Zugriff auf diese Einstellungen zu erhalten.
8. Wählen Sie bei **Art der Wiederherstellung**, ob Acronis Active Restore (S. 352) während der Wiederherstellung verwendet werden soll.
9. Spezifizieren Sie bei Bedarf noch weitere Einstellungen des Recovery-Tasks.

12.4.1.1 Aktionen nach Wiederherstellung einer Masterdatenbank

Die **Master**-Datenbank nimmt die Informationen über alle Datenbanken der Instanz auf. Daher enthält die **Master**-Datenbank in einem Backup Informationen über die Datenbanken, die zum Zeitpunkt des Backups in der Instanz vorlagen.

Nach Wiederherstellung der **Master**-Datenbank müssen Sie möglicherweise Folgendes tun:

- Datenbanken, die in der Instanz aufgetaucht sind, nachdem das Backup erstellt wurde, sind für die Instanz nicht sichtbar. Um diese Datenbanken zurück in die Produktion zu bringen, müssen Sie manuell an die Instanz anschließen. Anweisungen, wie Sie dies mit dem SQL Server Management Studio durchführen können, finden Sie im Abschnitt 'SQL Server-Datenbanken anfьgen (S. 331)'.
- Datenbanken, die nach Erstellung des Backups gelöscht wurden, werden in der Instanz als offline angezeigt. Löschen Sie diese Datenbanken mithilfe des SQL Server Management Studios.

12.4.1.2 Der Einsatz von Acronis Active Restore zur SQL-Datenbankwiederherstellung

Active Restore ist eine proprietäre Technologie von Acronis. Sie ermöglicht es, eine Microsoft SQL-Datenbank innerhalb von Minuten nach dem Start einer Datenbankwiederherstellung online zu

bringen. Dadurch können Benutzer bereits auf Ihre Daten zugreifen, noch während die Datenbank wiederhergestellt wird. Die Verwendung von Active Restore macht daher Sinn, wenn Sie die Datenbanken in das Stadium **Verwendungsbereit** oder **Schreibgeschützt** wiederherstellen.

Active Restore unterstützt folgende Backup-Speicherorte:

- Einen lokalen Ordner auf der Maschine, auf der die Wiederherstellung durchgeführt wird (ausgenommen optische Medien).
- Acronis Secure Zone.
- Eine Netzwerkfreigabe.

Um Active Restore verwenden zu können, müssen Sie es auf der Seite **Daten wiederherstellen** (S. 146) (bei **Art der Wiederherstellung**) aktivieren.

Der Recovery-Prozess

1. Falls der Recovery-Task die **Master**-Datenbank beinhaltet, wird diese zuerst wiederhergestellt. Während dieses Prozesses ist die Instanz im Einzelbenutzermodus, so dass Benutzer nicht mit ihr verbunden werden können. Nachdem die Datenbank wiederhergestellt wurde, startet die Software die Instanz neu.
2. Der Agent startet die Wiederherstellung von anderen Datenbanken. Mehrere Datebanken werden parallel wiederhergestellt.

   Zuerst sind die Datenbanken im Status **Wiederherstellen** und Benutzer haben keinen Zugriff auf diese. Nach einer kurzen Zeit erhalten die Benutzer 'Lese/Schreib'- oder 'Nur Lesen'-Zugriff auf die Datenbanken, abhängig vom in den Einstellungen des Recovery-Tasks spezifizierten Status.

   Details: Der Acronis Active Restore-Treiber fängt Benutzeranfragen ab. Die zur Erfüllung der Anforderungen benötigten Daten werden mit höchster Priorität wiederhergestellt, alle weiteren dagegen im Hintergrund. Als Resultat können Benutzer auf Ihre Daten zugreifen, obwohl die Datenbanken noch nicht vollständig wiederhergestellt sind.
3. Nach Abschluss der Wiederherstellung werden die Datenbanken neu angebunden. Das benötigt weniger als eine Minute.

Da die Erfüllung solcher Anforderungen simultan zur Wiederherstellung erfolgt, kann der Datenbankvorgang ausgebremst werden – auch dann, wenn in den Recovery-Optionen die Recovery-Prioritдt (S. 189) auf **Niedrig** eingestellt wurde. Obwohl die Datenbankausfallzeit minimal ist, kann es während der Wiederherstellung zu einer verringerten Performance kommen.

12.4.2 Datenbankdateien zu Ordnern extrahieren

SQL-Datenbankdateien und Transaktionsprotokolle können von einem Single-Pass-Backup zu einem von Ihnen spezifizierten Ordner extrahiert werden. Dies kann nützlich sein, wenn Sie Datenbanken zu einer Maschine wiederherstellen müssen, auf der kein Agent für SQL (Single-Pass) installiert ist oder Sie Daten zur Überwachung oder weiteren Verarbeitung durch Dritthersteller-Tools extrahieren müssen.

So extrahieren Sie Datenbankdateien

Auf der Seite **Daten wiederherstellen**:

1. Klicken Sie unter **Recovery-Quelle** auf **Daten wählen** und bestimmen Sie die entsprechenden Datenbanken.
2. Sollte die Konsole mit dem Management Server verbunden sein, dann wählen Sie eine registrierte Maschine, auf der der Agent für SQL (Single-Pass) installiert ist. Ansonsten können Sie diesen Schritt überspringen.

3. Wählen Sie **Datenbankdateien zu Ordnern extrahieren**.
4. Spezifizieren Sie bei **Zielordner** den Ordner, in dem die Datenbankdateien gespeichert werden sollen.

   Details: Wenn Sie mehr als eine Datenbank wählen, dann werden die Dateien jeder Datenbank in einem separaten Ordner innerhalb des von Ihnen spezifizierten Ordners extrahiert. Sollte der Zielordner bereits eine Datei oder Datenbank gleichen Namens wie die gewählte Datenbank enthalten, dann werden die Datenbankdateien zu einem Unterordner mit der Bezeichnung<Instanzname>\<Datenbankname> extrahiert.
5. Spezifizieren Sie bei Bedarf noch weitere Einstellungen des Recovery-Tasks.

Sobald die Extraktion abgeschlossen ist, können Sie die Datenbank an eine SQL Server-Instanz anschließen. Anweisungen, wie Sie dies mit dem SQL Server Management Studio durchführen können, finden Sie im Abschnitt 'SQL Server-Datenbanken anfьgen (S. 331)'.

12.5 SQL Server-Datenbanken von einem Single-Pass-Backup mounten

Wenn Sie eine SQL-Datenbank aus einem Backup mounten, wird diese temporär an Ihren SQL Server im 'Nur Lesen'-Modus angeschlossen. Sie können auf diese Datenbank genauso wie auf jede andere Datenbank der Instanz zugreifen.

Das Mounten von Datenbanken ist praktisch, wenn Sie eine der folgenden Aktionen durchführen wollen:

- Eine granuläre Wiederherstellung einzelner Datenbankobjekte, wie Tabellen, Datensätze, gespeicherte Prozeduren. Mounten Sie die Datenbank und verwenden Sie Dritthersteller-Tools, um die benötigten Informationen aus ihr abzurufen.
- Schnell auf zurückliegende Informationen zugreifen. Die Wiederherstellung einer großen Datenbank kann viel Zeit beanspruchen. Wenn Sie die Datenbank mounten, müssen Sie nicht warten, bis die Datenbank wiederhergestellt wurde.
- Das Stadium einer Datenbank zu einem bestimmten Zeitpunkt einsehen (beispielsweise zur Datengewinnung oder Überprüfung).

Die Mount-Aktion ist verfügbar, wenn die Konsole mit einer Maschine verbunden ist, auf der der Agent für SQL (Single-Pass) installiert ist. Das Single-Pass-Backup (Einzeldurchlauf-Backup) muss auf dieser Maschine in einem lokalen Ordner (ausgenommen optische Medien), in der Acronis Secure Zone oder auf einer Netzwerkfreigabe gespeichert sein. Andere Speicherorte werden von der Mount-Aktion nicht unterstützt.

Systemdatenbanken werden als Benutzerdatenbanken gemountet.

So mounten Sie eine SQL Server-Datenbank

1. Verbinden Sie die Konsole mit einer Maschine, auf der der Agent für SQL (Single-Pass) installiert ist.
2. Klicken Sie im Menü **Aktionen** auf den Befehl **SQL-Datenbanken von Image mounten**.
3. Klicken Sie auf **Daten wählen** und bestimmen Sie dann das Backup und die Datenbanken, die Sie mounten möchten.
4. Acronis Backup & Recovery 11.5 versucht die Zielinstanzen für die gewählten Datenbanken zu spezifizieren, indem es die ursprünglichen Pfade aus dem Backup nimmt. Falls die Zielinstanz für keine Datenbank ausgewählt ist oder falls Sie die Datenbank zu einer anderen Instanz mounten wollen, dann spezifizieren Sie die Zielinstanz manuell.

Sollten die Berechtigungen Ihres aktuellen Kontos nicht ausreichen, um auf die SQL Server-Zielinstanz zuzugreifen, dann werden Sie nach den Anmeldedaten gefragt.

5. Klicken Sie auf **OK**.

Eine gemountete Datenbank hat folgenden Namen: <ursprünglicher Datenbankname>**-Mounted**. Sollte eine Datenbank mit diesem Namen bereits existieren, dann wird die gemountete Datenbank folgendermaßen benannt: <ursprünglicher Datenbankname>**-Mounted (**<fortlaufende Nummer>**)**.

Beispiele: **MyDatabase-Mounted**, **MyDatabase-Mounted (2)**.

12.5.1 Gemountete SQL Server-Datenbanken trennen

Gemountete Datenbanken im System zu belassen, benötigt einiges an System-Ressourcen. Es ist daher empfehlenswert, dass Sie eine Datenbank, nachdem alle notwendigen Aktionen abgeschlossen wurden, wieder trennen (unmounten). Falls Sie eine Datenbank nicht manuell trennen, bleibt sie solange gemountet, bis das Betriebssystem oder der Agenten-Dienst neu gestartet wird.

So trennen (unmounten) Sie eine SQL-Datenbank

1. Verbinden Sie die Konsole mit einer Maschine, auf der der Agent für SQL (Single-Pass) installiert ist.
2. Klicken Sie im Fensterbereich **Navigation** auf **Gemountete SQL-Datenbanken verwalten**.
3. Um eine einzelne Datenbank abzuschalten (zu unmounten), wählen Sie diese aus und klicken Sie dann auf den Befehl **Trennen**. Um alle gemounteten Datenbanken gleichzeitig abzuschalten, klicken Sie auf **Alle trennen**.

   Sollte die gewählte Datenbank gerade verwendet werden, dann trennt Acronis Backup & Recovery 11.5 alle Benutzer zwangsweise von der Datenbank und führt dann die Trennung (Unmounting) durch.

12.6 Geclusterte SQL Server-Instanzen und AAG schützen

SQL Server-Hochverfügbarkeitslösungen

Die 'Windows Server Failover Clustering'-Funktionalität (WSFC) ermöglicht Ihnen, einen hochverfügbaren SQL Server durch Redundanz auf Instanzebene (Failover Cluster-Instanz, FCI) oder auf Datenbankebene (AlwaysOn-Verfügbarkeitsgruppe, AAG) zu konfigurieren. Sie können auch beide Methoden kombinieren.

In einer Failover Cluster-Instanz befinden sich die SQL-Datenbanken auf einem gemeinsam genutzten Storage. Weil auf diesen Storage nur vom aktiven Knoten aus Zugriff besteht, werden die SQL Server-Daten nur dann gesichert, wenn ein Backup des aktiven Knotens erstellt wird. Aus dem gleichen Grund können die SQL-Datenbanken nur auf einem aktiven Knoten wiederhergestellt werden. Hat der aktive Knoten einen Fehler, dann kommt es zu einem Failover und ein anderer Knoten wird aktiv.

In einer Verfügbarkeitsgruppe liegt jedes Datenbankreplikat auf einem anderen Knoten. Ist das primäre Replikat nicht mehr verfügbar, dann wird einem zweiten Replikat, das auf einem anderen Knoten liegt, die primäre Rolle zugewiesen.

Andere Lösungen beinhalten Datenbankspiegelung und Protokollversand. Weitere Informationen zu Lösungen mit hoher Verfügbarkeit für SQL Server finden Sie in der Microsoft-Dokumentation: http://msdn.microsoft.com/de-de/library/ms190202.aspx.

Für hohe Verfügbarkeit konfigurierte SQL Server per Backup sichern

Sowohl bei der FCI- wie auch bei der AAG-Lösung reicht es nicht aus, nur einen Knoten per Backup zu sichern. Falls dieser Knoten ausfällt, funktioniert der SQL Server zwar noch weiterhin, aber seine Datenbanken werden nicht mehr gesichert. Falls Sie ein unterbrechungsfreies Backup der SQL Server-Daten wünschen (egal wie viele Knoten verfügbar und betriebsbereit sind), dann sollten Sie folgenden Ansatz erwägen.

1. Installieren Sie den Agenten für SQL (Single-Pass) auf allen WSFC-Knoten.
2. Erstellen Sie auf jedem Knoten einen Backup-Plan mit identischen Einstellungen. Falls Sie eine Advanced-Edition von Acronis Backup & Recovery 11.5 haben, dann erstellen Sie einen einzelnen zentralen Backup-Plan für all diese Knoten.

   Die Einstellungen sind wie folgt:

   Klicken Sie bei **Backup-Quelle** auf **Elemente für das Backup** und aktivieren Sie das Kontrollkästchen neben der Maschine (nicht neben den einzelnen Laufwerken). Das gewährleistet, dass die gemeinsam genutzten Storages in dem Backup enthalten sind, wenn der Knoten aktiv wird.

   Spezifizieren Sie bei **Backup-Ziel** einen einzelnen Speicherort für alle Knoten. Das kann ein zentrales Depot oder auch einfach nur einen Netzwerkfreigabe sein. Das gewährleistet, dass alle Backup-Daten an einem Speicherort gesichert werden.

   Single-Pass-Laufwerk- und Anwendungs-Backup - Aktiviert.
3. Spezifizieren Sie bei Bedarf noch weitere Einstellungen des Backup-Plans.

Mit diesen Einstellungen werden die SQL-Datenbanken bei Auftreten eines Failovers auch auf einem anderen Knoten weiterhin per Backup gesichert. Wenn eine Datenwiederherstellung ansteht, finden Sie die Datenbanken in der **Datenanzeige** oder **Archiv-Anzeige** des Depots – und zwar unter dem Knoten, von dem aus das Backup erfolgte.

Für hohe Verfügbarkeit konfigurierte Datenbanken wiederherstellen

Eine für Spiegelung konfigurierte oder in einer AlwaysOn-Verfügbarkeitsgruppe (AAG) enthaltene Datenbank kann während einer Wiederherstellung nicht überschrieben werden, weil der Microsoft SQL Server dies verhindert. Sie müssen die Spiegelung der Zieldatenbank entfernen oder die Zieldatenbank von der AlwaysOn-Verfügbarkeitsgruppe (AAG) ausschließen, bevor Sie die Wiederherstellung durchführen. Oder Sie stellen die Datenbank einfach als 'Nicht-AGG'-Datenbank wieder her. Nach Abschluss der Wiederherstellung können Sie die ursprüngliche Spiegelung/AAG-Konfiguration wieder aufbauen.

13 Das Microsoft Active Directory mit Single-Pass-Backups schützen

Dieser Abschnitt beschreibt, wie Sie Single-Pass-Laufwerk- und Anwendungs-Backups verwenden, um die Rolle 'Active Directory-Domänendienste' des Microsoft Active Directorys zu schützen.

Die Single-Pass-Backup-Funktionalität steht Ihnen zur Verfügung, wenn Sie den Acronis Backup & Recovery 11.5 Agenten für Microsoft Active Directory (Single-Pass) installieren. Der Agent wird in diesem Dokument auch als Agent für Active Directory (Single-Pass) bezeichnet.

Ohne diesen Agenten können Sie Ihre Active Directory-Daten mithilfe von Backups auf Laufwerksebene schützen. Eine detaillierte Beschreibung dieser Methode finden Sie im Abschnitt 'Anwendungen mit Laufwerk-Backups schützen (S. 318)'.

13.1 Agent für Active Directory (Single-Pass)

Der Agent für Active Directory (Single-Pass) erstellt ein applikationskonformes Laufwerk-Backup, welches auch als Single-Pass-Backup oder Einzeldurchlauf-Backup bezeichnet wird. Während eines Backups fügt der Agent für Active Directory (Single-Pass) der resultierenden Backup-Datei bestimmte Microsoft Active Directory-Metadaten hinzu.

Der Agent ermöglicht es Ihnen, Active Directory-Dateien von bzw. aus einem Single-Pass-Backup zu extrahieren, ohne dass dabei komplette Laufwerke oder Volumes wiederhergestellt werden müssen. Danach können Sie die beschädigten Dateien durch die extrahierten Dateien ersetzen.

Der Domain-Controller kann außerdem auch als Ganzes wiederhergestellt werden.

13.2 Unterstützte Betriebssysteme

Der Agent für Active Directory (Single-Pass) kann auf folgenden Betriebssystemen installiert werden:

- Windows Server 2003/2003 R2 – Standard und Enterprise Editionen (x86, x64)
- Windows Small Business Server 2003/2003 R2
- Windows Server 2008 – Standard, Enterprise und Datacenter Editionen (x86, x64)
- Windows Small Business Server 2008
- Windows Server 2008 R2 – Standard, Enterprise, Datacenter und Foundation Editionen
- Windows Small Business Server 2011 – alle Editionen
- Windows Server 2012/2012 R2 – alle Editionen

13.3 Installation des Agenten für Active Directory (Single-Pass)

Der Agent für Active Directory (Single-Pass) kann nur auf einem Domain-Controller installiert werden. Eine Remote-Installation des Agenten ist nicht möglich.

Der Agent ist in den Setup-Programmen der Standalone- und Advanced-Editionen von Acronis Backup & Recovery 11.5 enthalten. Die vom Agenten bereitgestellte Funktionalität ist in beiden Setup-Programmen gleich.

Der Agent für Active Directory (Single-Pass) wird als Add-on des Agenten für Windows installiert.

Erforderliche Lizenzen

Verwenden Sie zur Installation des Agenten für Windows eine beliebige Lizenz, die es ermöglicht, den Agenten zu installieren.

Falls der Agenten für Windows mit einer Advanced Server SBS Edition-Lizenz installiert wird, können Sie den Agenten für Active Directory (Single-Pass) ohne eine zusätzliche Lizenz installieren. Verwenden Sie ansonsten die folgendene Lizenz: Acronis Backup & Recovery 11.5 Microsoft Active Directory Add-on.

Diese Lizenz ermöglicht Ihnen die Installation des Agenten für Active Directory (Single-Pass) auf einem physikalischen Host und auf vier virtuellen Maschinen, die auf demselben Host laufen. Beachten Sie, dass zusammen mit dem Agenten für Active Directory (Single-Pass) auf jeder virtuellen Maschine auch der Agent für Windows installiert werden muss.

Zur Verwendung des Produktes im Testmodus benötigen Sie keine Lizenzen.

Installation

Installieren Sie den Agenten auf gleiche Weise wie den Agenten für Windows. Detaillierte Schritt-für-Schritt-Anweisungen finden Sie in folgenden Abschnitten der Installationsanleitung:

- 'Interaktive Installation in den Standalone-Editionen'.
- 'Interaktive Installation in den Advanced-Editionen'.

13.4 Microsoft Active Directory per Backup sichern

Um das Active Directory schützen zu können, erstellen Sie einen Backup-Plan – oder Sie verwenden die Funktion **Backup jetzt** (wie im Abschnitt 'Backup (S. 58)' beschrieben).

Folgen Sie den empfohlenen, optimalen Vorgehensweisen, die im Abschnitt 'Active Directory-Backup (S. 328)' beschrieben sind.

Stellen Sie sicher, dass die Backup-Option Volume Shadow Copy Service (S. 142) auf **Volume Shadow Copy Service verwenden** eingestellt ist – und dass der ausgewählte Snapshot-Provider nicht auf **Software - Acronis VSS Provider** steht. Die beste Wahl ist **Software – System-Provider**.

13.5 Microsoft Active Directory wiederherstellen

Einen Domain-Controller wiederherstellen

Orientieren Sie sich an einem der folgenden Abschnitte, wenn der Domain-Controller nicht mehr booten kann (abhängig von der Anzahl und Verfügbarkeit von Domain-Controllern in Ihrer Umgebung):

- 'Einen Domain Controller wiederherstellen (andere DCs sind verfьgbar) (S. 334)'.
- 'Einen Domain Controller wiederherstellen (es sind keine anderen DCs verfьgbar) (S. 336)'.

Active Directory-Daten wiederherstellen

Sollten die Active Directory-Datenbankdateien oder der SYSVOL-Ordner beschädigt sein, dafür aber der Domain-Controller noch im normalen Modus starten können, dann können Sie nur die Active Directory-Daten wiederherstellen.

Verwenden Sie eine der nachfolgenden Methoden:

- 'Нцherstufen des Domain-Controllers' (S. 358)

  Dies ist lediglich eine Replikation aller Active Directory-Daten von anderen DCs.
- 'Active Directory-Daten von einem Single-Pass-Backup wiederherstellen' (S. 359)

  Diese Methode ermöglicht Ihnen eine Wiederherstellung aller Active Directory-Daten – unabhängig von der Verfügbarkeit anderer DCs. Falls andere DCs verfügbar sind, können Sie eine autorisierte Wiederherstellung von einzelnen, bestimmten Active Directory-Objekten durchführen. Sie können beispielsweise ein unbeabsichtigt gelöschtes Benutzerkonto oder Computerkonto wiederherstellen. Andere Objekte werden von anderen DCs her repliziert.

13.5.1 Höherstufen des Domain-Controllers

Diese Wiederherstellungsmethode ist nur dann verfügbar, falls die Domain noch andere Domain-Controller hat. Die Verfügbarkeit eines Backups ist nicht erforderlich.

Verwenden Sie, um das Microsoft Active Directory wiederherzustellen, das Tool **Dcpromo**, um damit den Domain-Controller mit den beschädigten Daten zuerst tieferzustufen – und dann erneut, um diesen Domain-Controler wieder höherzustufen.

Fühlen Sie folgende Befehle aus, um den Domain-Controller erneut höherzustufen:

```
dcpromo /forceremoval
dcpromo /adv
```

13.5.2 Active Directory-Daten von einem Single-Pass-Backup wiederherstellen

Diese Art der Datenwiederherstellung kann unabhängig davon verwendet werden, ob die Domain noch weitere Domain-Controller hat.

Dieser Abschnitt beschreibt nur die Schritte und Einstellungen, die zur Wiederherstellung von Active Directory-Daten von einem Single-Pass-Backup (Einzeldurchlauf-Backup) spezifisch sind. Die allgemeinen Einstellungen eines Recovery-Tasks sind im Abschnitt 'Einen Recovery-Task erstellen (S. 146)' beschrieben.

Die Active Directory-Daten extrahieren

Auf der Seite **Daten wiederherstellen**:

1. Klicken Sie bei **Recovery-Quelle** auf **Daten wählen**. Wählen Sie die Daten und den Recovery-Punkt.

   Warnung! *– Sollte die Domain über zwei oder mehr Domain-Controller verfügen, dann wählen Sie einen Recovery-Punkt, der nicht älter als die sogenannte 'Tombstone-Lebensdauer' ist. Anderenfalls kann es zu Problemen bei der Replikation kommen.*

2. Sollte die Konsole mit dem Management Server verbunden sein, dann wählen Sie eine registrierte Maschine, auf welcher der Agent für Active Directory (Single-Pass) installiert ist. Ansonsten können Sie diesen Schritt überspringen.
3. Klicken Sie auf **Ziel** und wählen Sie einen Ordner oder Netzwerkordner, in dem die Microsoft Active Directory-Daten als Dateien extrahiert werden sollen. Die Datenbankdateien und der SYSVOL-Ordner werden unter Neuerstellung eines vollständigen Pfades wiederhergestellt.
4. Wählen Sie bei **Überschreiben**, ob bereits existierende Dateien, die den gleichen Namen wie im Archiv haben, überschrieben werden sollen.
5. Spezifizieren Sie bei Bedarf noch weitere Einstellungen des Recovery-Tasks (S. 146).
6. Starten Sie den Recovery-Task und warten Sie, bis er abgeschlossen ist.

Active Directory-Daten durch die extrahierten Dateien ersetzen

1. Starten Sie den Domain-Controller neu und drücken Sie während des Startvorgangs auf F8.
2. Wählen Sie im Fenster **Erweiterte Startoptionen** das Element **Verzeichnisdienst-Wiederherstellungsmodus**.
3. [Optional] Erstellen Sie eine Kopie der aktuellen Active Directory-Datenbankdateien, falls die Änderungen wieder rückgängig gemacht werden sollen.
4. Verschieben Sie die extrahierten Active Directory-Daten zu ihrem ursprünglichen Speicherort:
   a. Gehen Sie zu dem Ordner mit den extrahierten Daten. Dieser Ordner enthält einen oder mehrere Ordner. Die Namen dieser Ordner enthalten Laufwerksbuchstaben derjenigen Laufwerke, auf denen die gesicherten Active Directory-Daten gespeichert waren. Beispielsweise **Laufwerk(C)**.

b. Kopieren Sie die Inhalte von jedem dieser Ordner in das Stammverzeichnis des entsprechenden Festplattenlaufwerkes. Kopieren Sie beispielsweise die Inhalte des Ordners **Laufwerk(C)** auf Laufwerk **C:** (bzw. in dessen Stammverzeichnis) – und die Inhalte des Ordners **Laufwerk(E)** auf das Laufwerk **E:**. Wählen Sie bei entsprechender Nachfrage, dass die Dateien überschrieben werden.

Die Wiederherstellung abschließen

1. Falls die Domain nur einen Domain-Controller hat, dann überspringen Sie diesen Schritt. Wählen Sie ansonsten eine der nachfolgenden Varianten:
   - Falls Sie die komplette Active Directory-Datenbank wiederherstellen wollen, dann führen Sie die Schritte 3-8 durch, wie es unter 'USN-Rollback' im Abschnitt 'Vermeidung eines USN-Rollbacks (S. 338)' beschrieben ist.
   - Falls Sie einzelne Objekte wiederherstellen wollen (wie beispielsweise versehentlich gelöschte Benutzer- oder Computerkonten), dann führen Sie die Schritte 2-4 durch, wie es im Abschnitt 'Wiederherstellung versehentlich gelцschter Informationen (S. 337)' beschrieben ist.
2. Starten Sie den Domain-Controller im normalen Modus neu.
3. Stellen Sie sicher, dass der Active Directory-Dienst erfolgreich gestartet wurde.

14 Eine verwaltete Maschine administrieren

In diesem Abschnitt werden die Ansichten beschrieben, die über den Verzeichnisbaum 'Navigation' einer mit der Konsole verbundenen verwalteten Maschine verfügbar sind und erklärt, wie Sie mit diesen Ansichten arbeiten. In diesem Abschnitt werden außerdem zusätzliche Aktionen behandelt, die auf einer verwalteten Maschine ausgeführt werden können – wie das Wechseln einer Lizenz, das Einstellen der **Maschinen-Optionen** oder das Einsammeln von Systeminformationen.

14.1 Backup-Pläne und Tasks

Die Ansicht **Backup-Pläne und Tasks** informiert Sie über die Datensicherung auf einer bestimmten Maschine. Sie ermöglicht Ihnen, Backup-Pläne und Tasks zu überwachen und zu verwalten.

Sehen Sie unter Backup-Plan-Ausfьhrungsstadium (S. 363) nach, um herauszufinden, was ein Backup-Plan auf einer Maschine gerade tut. Das Ausführungsstadium eines Backup-Plans entspricht dem kumulativen Stadium all seiner jüngsten Aktivitäten. Der Status eines Backup-Plans (S. 364) hilft Ihnen bei der Einschätzung, ob die Daten erfolgreich gesichert wurden.

Um den aktuellen Fortschritt eines Tasks im Überblick zu behalten, verfolgen Sie sein Stadium (S. 365). Prüfen Sie den Status (S. 365) eines Tasks, um sein Ergebnis in Erfahrung zu bringen.

Typischer Arbeitsablauf

- Nutzen Sie Filter, um in der Backup-Plan-Tabelle die gewünschten Backup-Pläne (Tasks) zu sehen. Standardmäßig zeigt die Tabelle die Pläne der verwalteten Maschine nach Namen sortiert an. Sie können außerdem nicht benötigte Spalten ausblenden bzw. ausgeblendete wieder aktivieren. Zu Details siehe 'Tabellenelemente sortieren, filtern und konfigurieren (S. 29)'.
- Wählen Sie in der Backup-Tabelle den Backup-Plan (Task).
- Verwenden Sie die Schaltflächen der Symbolleiste, um eine Aktion auf den gewählten Plan (Task) anzuwenden. Zu Details siehe 'Aktionen fьr Backup-Plдne und Tasks (S. 361)'.
- Verwenden Sie den Bereich 'Informationen' im unteren Teil des Fensters, um detaillierte Informationen über den gewählten Plan (Task) einsehen zu können. Die Leiste ist standardmäßig

eingeklappt. Sie können den Fensterbereich aufklappen, indem Sie auf das Pfeilsymbol klicken. Der Inhalt der Leiste wird außerdem auch in den Fenstern **Plan-Details** (S. 370) und **Task-Details** (S. 372) angezeigt.

14.1.1 Aktionen für Backup-Pläne und Tasks

Nachfolgend finden Sie eine Anleitung zur Durchführung von Aktionen für Backup-Pläne und Tasks.

Einschränkungen

- Ohne administrative Berechtigungen kann ein Benutzer auf einer Maschine keine zu anderen Benutzern gehörenden Pläne oder Tasks ausführen oder modifizieren.
- Es ist nicht möglich, einen aktuell laufenden Backup-Plan oder Task zu modifizieren oder zu löschen.
- Ein zentraler Backup-Plan oder Task kann nur auf Seiten des Management Servers modifiziert oder gelöscht werden.

Aufgabe	**Lösung**
Einen neuen Backup-Plan oder Task erstellen	Klicken Sie auf **Neu** und wählen Sie eine der folgenden Optionen: ▪ Backup-Plan (S. 58) ▪ Recovery-Task (S. 146) ▪ Validierungstask (S. 266)
Details eines Plans/Tasks einsehen	Klicken Sie auf **Details**. Überprüfen Sie im entsprechenden Fenster **Plan-Details** (S. 370) oder **Task Details** (S. 372) die entsprechenden Angaben.
Log eines Plans/Tasks einsehen	Klicken Sie auf **Log**. Sie gelangen dadurch in die Ansicht **Log** (S. 372), die eine Liste von Log-Einträgen enthält, die in Bezug auf die Plan-/Task-Aktivitäten gruppiert sind.
Einen Plan/Task ausführen	**Backup-Plan** 1. Klicken Sie auf **Ausführen**. 2. Wählen Sie aus dem Listenfeld den Task des Plans aus, den Sie ausführen müssen. Die Ausführung des Backup-Plans startet auch unmittelbar den dazugehörigen, ausgewählten Task, ungeachtet seiner Planung und anderer Konditionen. **Task** Klicken Sie auf **Ausführen**. Die Ausführung des Tasks startet unmittelbar, ungeachtet seiner Planung und anderer Bedingungen.

Aufgabe	Lösung
Einen Plan/Task stoppen	Klicken Sie auf **Stopp**. **Backup-Plan** Einen laufenden Backup-Plan zu stoppen bedeutet auch, alle seine Tasks zu stoppen. Folglich werden alle Task-Aktionen abgebrochen. **Task** Das Stoppen eines Tasks führt zum Abbruch seiner jeweiligen Aktion (Recovery, Validierung, Export, Konvertierung etc.). Der Task wechselt in das Stadium **Inaktiv**. Die Task-Planung bleibt aber, sofern erstellt, weiter gültig. Um die Aktion abzuschließen, müssen Sie den Task erneut ausführen. **Was passiert, wenn Sie einen Recovery-Task stoppen?** ▪ Wiederherstellung von Laufwerken: Die abgebrochene Aktion kann zu Veränderungen auf dem Ziellaufwerk führen. In Abhängig von der seit Task-Ausführung verstrichenen Zeit ist das Ziellaufwerk möglicherweise nicht initialisiert, der Speicherplatz nicht zugeordnet oder wurden einige Volumes wiederhergestellt, andere jedoch nicht. Führen Sie den Task erneut aus, um das komplette Laufwerk wiederherzustellen. ▪ Wiederherstellung von Volumes: Das Ziel-Volume wird gelöscht und der entsprechende Speicherplatz wird 'nicht zugeordnet' – das gleiche Ergebnis, wie beim Fehlschlagen einer Wiederherstellung. Führen Sie den Task erneut aus, um das verlorene Volume wiederherzustellen. ▪ Wiederherstellung von Dateien und Ordnern: Die abgebrochene Aktion kann zu Veränderungen im Zielordner führen. In Abhängig von der seit Task-Ausführung verstrichenen Zeit wurden einige Dateien möglicherweise wiederhergestellt, andere wiederum nicht. Führen Sie den Task erneut aus, um alle Dateien wiederherzustellen.
Einen Plan/Task editieren	Klicken Sie auf **Bearbeiten**. Die Bearbeitung eines Backup-Plans wird auf dieselbe Art durchgeführt wie das Erstellen (S. 58), mit Ausnahme folgender **Einschränkungen**: Beim Bearbeiten eines Backup-Plans ist es nicht immer möglich, alle Optionen für Backup-Schemata zu verwenden, falls das erstellte Archiv nicht leer ist (d.h. Backups enthält). 1. Es ist nicht möglich, das Schema zu 'Großvater-Vater-Sohn' oder 'Türme von Hanoi' zu ändern. 2. Sie können die Zahl der Level nicht ändern, falls das Schema 'Türme von Hanoi' verwendet wird. In allen anderen Fällen kann das Schema verändert werden und sollte so weiterarbeiten, als wären bereits existierende Archive durch ein neues Schema erstellt worden. Bei leeren Archiven sind alle Veränderungen möglich.
Einen Backup-Plan klonen	Klicken Sie auf **Klonen**. Der Klon des ursprünglichen Backup-Plans wird mit dem Standardnamen '*Klon von <ursprünglicher Plan-Name>*' erstellt. Der geklonte Plan wird unmittelbar nach dem Klonvorgang deaktiviert, damit er nicht gleichzeitig mit dem ursprünglichen Plan ausgeführt wird. Sie können die Einstellungen des geklonten Plans bearbeiten, bevor Sie ihn dann aktivieren.
Einen Plan aktivieren	Klicken Sie auf **Aktivieren**. Der zuvor deaktivierte Backup-Plan wird wieder neu gemäß seiner Planung ausgeführt.

Aufgabe	Lösung
Einen Plan deaktivieren	Klicken Sie auf **Deaktivieren**. Der Backup-Plan wird nicht mehr gemäß seiner Planung ausgeführt. Er kann jedoch manuell gestartet werden. Der Plan verbleibt ansonsten auch nach einer manuellen Ausführung deaktiviert. Der Plan wird wieder wie normal ausgeführt, wenn Sie ihn erneut aktivieren.
Einen Plan exportieren	Klicken Sie auf **Exportieren**. Spezifizieren Sie Pfad und Namen für die resultierende Datei. Zu weiteren Informationen siehe 'Export und Import von Backup-Plдnen (S. 366)'.
Einen Plan importieren	Klicken Sie auf **Importieren**. Spezifizieren Sie den Pfad und Namen der Datei, die einen zuvor exportierten Plan enthält. Zu weiteren Informationen siehe 'Export und Import von Backup-Plдnen (S. 366)'.
Einen Plan/Task löschen	Klicken Sie auf **Löschen**.

14.1.2 Stadien und Statuszustände von Backup-Plänen und Tasks

14.1.2.1 Ausführungsstadien von Backup-Plänen

Das Stadium eines Backup-Plans entspricht dem kumulativen Stadium aller Tasks/Aktivitäten dieses Plans.

	Stadium	Wie es bestimmt wird	Handhabung
1	**Benutzereingriff erforderlich**	Wenigstens ein Task erfordert einen Benutzereingriff. Siehe anderenfalls Punkt 2.	Identifizieren Sie die Tasks, die eine Interaktion erfordern (das Programm zeigt an, was zu tun ist) –> Stoppen Sie die betreffenden Tasks oder ermöglichen Sie ihre Ausführung (wechseln Sie das Medium, sorgen Sie für zusätzlichen Platz im Depot, ignorieren Sie Lesefehler, erstellen Sie eine fehlende Acronis Secure Zone).
2	**Läuft**	Wenigstens ein Task wird ausgeführt. Siehe anderenfalls Punkt 3.	Es ist keine Handlung nötig.

3	**Wartend**	Wenigstens ein Task befindet sich in Wartestellung. Siehe anderenfalls Punkt 4.	Warten auf Bedingung. Diese Situation ist recht gängig, jedoch kann eine zu lange Backup-Verzögerung riskant sein. Die Lösung kann das Einstellen der maximalen Verzögerung (S. 141) sein, nach der der Task auf jeden Fall startet – oder dass Sie die entsprechende Bedingung erzwingen (beispielsweise dem betreffenden Benutzer zur Abmeldung auffordern oder eine benötigte Netzwerk-Verbindung einschalten). Wartend, während ein anderer Task die benötigten Ressourcen sperrt. Eine einmalige Wartesituation kann entstehen, wenn ein Task-Start verzögert wird oder eine Task-Ausführung aus bestimmten Gründen wesentlich länger als gewöhnlich dauert und daher einen anderen Task an der Ausführung hindert. Diese Situation wird automatisch gelöst, wenn der blockierende Task seinen Abschluss findet. Erwägen Sie, einen zu lange festhängenden Task zu stoppen, um dem nachfolgenden den Start zu ermöglichen. Eine andauernde Überlappung von Tasks kann das Ergebnis inkorrekt angelegter Zeit- bzw. Backup-Pläne sein. In solchen Fällen macht es natürlich Sinn, den entsprechenden Plan zu editieren.
4	**Untätig**	Alle Tasks befinden sich in Ruhestellung.	Es ist keine Handlung nötig.

14.1.2.2 Backup-Plan-Statuszustände

Ein Backup-Plan kann einen von folgenden Statuszuständen haben: **Fehler, Warnung, OK**.

Der Status eines Backup-Plans ergibt sich aus den Ergebnissen, die die Tasks/Aktivitäten dieses Plans bei ihren letzten Ausführungen gemeldet haben.

	Status	**Wie es bestimmt wird**	**Handhabung**
1	**Fehler**	Wenigstens ein Task ist fehlgeschlagen. Siehe anderenfalls Punkt 2.	Identifizieren Sie die fehlgeschlagenen Tasks –> Überprüfen Sie die Task-Ereignismeldungen im Log, um die Fehlerursache zu ermitteln und setzen Sie dann eine oder mehrere der nachfolgenden Lösungen um: ▪ Entfernen Sie die Fehlerursache –> [optional] Starten Sie den fehlgeschlagenen Task manuell ▪ Bearbeiten Sie den lokalen Plan, falls der Fehler bei ihm lag, um sein zukünftiges Versagen zu verhindern. ▪ Bearbeiten Sie den zentralen Backup-Plan auf dem Management Server, falls es ein zentraler Plan war, der fehlgeschlagen ist.
2	**Warnung**	Wenigstens ein Task wurde mit Warnungen abgeschlossen. Siehe anderenfalls Punkt 3.	Prüfen Sie das Log, um die Warnungen zu lesen –> [optional] Führen Sie Aktionen aus, um zukünftige Warnungen bzw. Fehler zu verhindern.
3	**OK**	Alle Tasks wurden erfolgreich abgeschlossen.	Es ist keine Handlung nötig. Beachten Sie, dass ein Backup-Plan 'OK' sein kann, wenn bisher keiner der Tasks gestartet wurde.

14.1.2.3 Task-Stadien

Ein Backup-Task kann sich in einem der folgenden Stadien befinden: **Untätig**; **Wartend**; **Läuft**; **Benutzereingriff erforderlich**. Das anfängliche Task-Stadium ist **Untätig**.

Sobald der Task manuell gestartet wurde oder das als Auslöser spezifizierte Ereignis eingetreten ist, wechselt der Task entweder in das Stadium **Läuft** oder **Wartend**.

Läuft

Ein Task wechselt in das Stadium **Läuft**, wenn das im Scheduler definierte Ereignis eintritt UND alle im Backup-Plan definierten Bedingungen zutreffen UND kein anderer Task läuft, der benötigte Ressourcen blockiert. In diesem Fall verhindert also nichts die Ausführung des Tasks.

Wartend

Ein Task wechselt in das Stadium **Wartend**, wenn er im Begriff ist zu starten und dabei jedoch bereits ein anderer, die gleichen Ressourcen benutzender Task ausgeführt wird. Das bedeutet, dass auf einer Maschine nicht mehr als ein Backup-Task gleichzeitig laufen kann. Genauso wenig ist es möglich, dass ein Backup- und ein Recovery-Task gleichzeitig laufen können, falls sie dieselbe Ressource verwenden. Sobald der andere Task die Ressource freigibt, wechselt der wartende Task in das Stadium **Läuft**.

Ein Task kann außerdem in das Stadium **Wartend** wechseln, wenn das im Scheduler spezifizierte Ereignis zwar erfolgt, jedoch die im Backup-Plan definierten Bedingungen nicht erfüllt sind. Zu Details siehe 'Task-Startbedingungen (S. 141)'.

Benutzereingriff erforderlich

Jeder laufende Task kann sich selbst in das Stadium **Benutzereingriff erforderlich** versetzen, falls eine Benutzerinteraktion nötig ist, wie etwa ein Medienwechsel oder das Ignorieren eines Lesefehlers. Das nächste Stadium kann **Untätig** sein (falls der Benutzer wählt, dass der Task gestoppt wird) oder **Läuft** (bei Wahl von 'Ignorieren/Wiederholen' oder einer anderen Handlung, etwa einem Neustart, die den Task in das Stadium **Läuft** versetzen kann).

14.1.2.4 Task-Statuszustände

Ein Task kann sich in einem von folgenden Statuszuständen befinden: **Fehler**; **Warnung**; **OK**.

Der Status eines Tasks wird aus dem Ergebnis der letzten Ausführung des Tasks ermittelt.

	Status	**Wie es bestimmt wird**	**Handhabung**
1	**Fehler**	Das letzte Ergebnis ist „Fehlgeschlagen“	Identifizieren Sie den fehlgeschlagenen Task –> Überprüfen Sie das Task-Log, um die Fehlerursache zu ermitteln, und setzen Sie dann eine oder mehrere der nachfolgenden Lösungen um: ▪ Entfernen Sie die Fehlerursache –> [optional] Starten Sie den fehlgeschlagenen Task manuell ▪ Bearbeiten Sie den fehlgeschlagenen Task, um zukünftiges Misslingen zu verhindern
2	**Warnung**	Das letzte Ergebnis ist „Mit Warnung abgeschlossen“ oder der Task wurde gestoppt.	Prüfen Sie das Log, um die Warnungen zu lesen –> [optional] Führen Sie Aktionen aus, um zukünftige Warnungen bzw. Fehler zu verhindern.

3	**OK**	Das letzte Ergebnis ist „Erfolgreich abgeschlossen“ oder „Noch nicht ausgeführt“	Das Stadium 'Noch nicht ausgeführt' bedeutet, dass der Task noch nie gestartet wurde, oder dass er bereits gestartet, jedoch noch nicht abgeschlossen wurde und daher sein Ergebnis noch nicht verfügbar ist. Sie können auf Wunsch herausfinden, warum der Task bisher noch nicht gestartet wurde.

14.1.3 Backup-Pläne exportieren und importieren

Die Export-Aktion erstellt eine Datei mit der kompletten Konfiguration des Backup-Plans. Sie können die Datei importieren, um so den exportierten Backup-Plan auf einer anderen Maschine erneut nutzen zu können.

Zentrale Backup-Pläne können nur von einem Management Server exportiert und nur in einen Management Server importiert werden.

Sie können die Pläne in der grafischen Benutzeroberfläche von Acronis Backup & Recovery 11.5 beim Importieren bearbeiten (oder auch später). Backup-Pläne werden in .xml-Dateien exportiert, so dass Sie die exportierten Dateien der Backup-Pläne (S. 367) auch mit einem Text-Editor bearbeiten können. Kennwörter werden in den exportierten Dateien verschlüsselt.

Anwendungsbeispiele

- **Neuinstallation des Agenten**

  Exportieren Sie die Backup-Pläne, bevor Sie den Agenten neu installieren – nach der Neuinstallation können Sie diese dann wieder importieren.

- **Deployment eines Backup-Plans auf mehrere Maschinen**

  Sie haben eine Umgebung, wo die Verwendung des Acronis Backup & Recovery 11.5 Management Servers nicht möglich ist, beispielsweise aufgrund von Sicherheitsbeschränkungen. Sie wollen nichtsdestotrotz denselben Backup-Plan auf mehreren Maschinen verwenden. Exportieren Sie den Plan von einer der Maschinen und verteilen Sie ihn als Datei (S. 369) auf die anderen Maschinen.

Anmeldedaten anpassen

Bevor Sie einen Backup-Plan exportieren, der später in einer anderen Maschine importiert wird, sollten Sie das Benutzerkonto überprüfen, unter dem der Plan läuft (**Bearbeiten** –> **Plan-Parameter** –> **Anmeldedaten des Tasks, Kommentare, Bezeichnung anzeigen** –> **Anmeldedaten des Plans**).

Der Plan wird auf einer anderen Maschine erfolgreich ausgeführt, falls der Wert für die **Anmeldedaten des Plans** entweder **Anmeldedaten des Acronis Service** lautet oder **Ausführen als: ... (Aktueller Benutzer)**. Falls der Parameter **Anmeldedaten des Plans** ein bestimmtes Benutzerkonto enthält, wird der Plan nur starten, wenn auf der betreffenden Maschine ein identisches Konto vorhanden ist. Sie müssen daher möglicherweise eine der folgenden Aktionen ausführen:

- Erstellen Sie ein Konto mit identischen Anmeldedaten auf der Maschine, auf der der Plan importiert wird.
- Bearbeiten Sie die Anmeldedaten in der exportierten Datei, bevor Sie diese importieren. Zu Details siehe die Exportdatei bearbeiten (S. 367).
- Bearbeiten Sie die Anmeldedaten nach Importieren des Plans.

Auszuführende Schritte

So exportieren Sie einen Backup-Plan

1. Wählen Sie einen Backup-Plan in der Ansicht **Backup-Pläne und Tasks**.

2. Klicken Sie auf **Exportieren**.
3. Spezifizieren Sie Pfad und Namen für die Exportdatei.
4. Bestätigen Sie Ihre Wahl.

So importieren Sie einen Backup-Plan

1. Klicken Sie in der Ansicht **Backup-Pläne und Tasks** auf **Importieren**.
2. Spezifizieren Sie Pfad und Namen für die Exportdatei.
3. Bestätigen Sie Ihre Wahl.
4. Falls Sie den neu importierten Backup-Plan bearbeiten müssen, dann wählen Sie ihn in der Ansicht **Backup-Pläne und Tasks** aus und klicken Sie dann auf **Bearbeiten**. Nehmen Sie alle notwendigen Änderungen vor und klicken Sie dann auf **Speichern**.

14.1.3.1 Die Exportdatei bearbeiten

Die Exportdatei ist eine .xml-Datei und kann daher mit einem Texteditor bearbeitet werden.

Und so können Sie einige nützliche Änderungen vornehmen.

So modifizieren Sie Anmeldedaten

In der Export-Datei enthalten die Tags **<login>** den Benutzernamen und die Tags **<password>** das Benutzerkennwort.

Ändern Sie zum Modifizieren der Anmeldedaten die Tags **<login>** und **<password>** in den entsprechenden Abschnitten:

- Anmeldedaten des Plans – der Abschnitt **<plan><options><common_parameters>**
- Anmeldedaten zum Zugriff auf die gesicherten Daten – der Abschnitt **<plan><targets><inclusions>**
- Anmeldedaten zum Zugriff auf das Backup-Ziel – der Abschnitt **<plan><locations>**.

Seien Sie besonders vorsichtig bei der Modifikation des Tags **<password>**. Das Tag, das ein verschlüsseltes Kennwort enthält, sieht aus wie **<password encrypted="true">...</password>**.

So ändern Sie das verschlüsselte Kennwort

1. Starten Sie in der Befehlszeile das Utility **acronis_encrypt**.

   acronis_encrypt UserPassword#1

   (hier ist **UserPassword#1** das Kennwort, das Sie verschlüsseln wollen).
2. Das Utility gibt einen String aus, beispielsweise '**XXXYYYZZZ888**'.
3. Kopieren Sie diesen String und fügen Sie ihn folgendermaßen in das Tag ein:

   <password encrypted="true">XXXYYYZZZ888</password>

Das Utility **acronis_encrypt** ist auf jeder Maschine verfügbar, auf der die Acronis Backup & Recovery 11.5 Management Console oder das Befehlszeilenwerkzeug von Acronis Backup & Recovery 11.5 (**acrocmd**) installiert ist. Der Pfad zum Utility ist folgender:

- In einer 32-Bit-Version von Windows: **%CommonProgramFiles%\Acronis\Utils**
- In einer 64-Bit-Version von Windows: **%CommonProgramFiles(x86)%\Acronis\Utils**
- In Linux: **/usr/sbin**

Einen Backup-Plan die Anmeldedaten des Agenten verwenden lassen

Löschen Sie vor Importieren oder Bereitstellen der Exportdatei den Wert des benötigten Tags **<login>**. Der importierte oder verteilte Plan wird dann die Anmeldedaten des Agenten-Dienstes verwenden.

Beispiel

Finden Sie, damit der Backup-Plan unter den Anmeldedaten des Agenten läuft, das Tag **<login>** im Abschnitt **<plan><options><common_parameters>**. Das Tag sieht folgendermaßen aus:

```
<login>
   Administrator
</login>
<password encrypted="true">
   XXXYYYZZZ888
</password>
```

Löschen Sie den Wert des Tags **<login>**, damit das Tag folgendermaßen aussieht:

```
<login>
</login>
<password encrypted="true">
   XXXYYYZZZ888
</password>
```

So ändern Sie die Elemente für ein Backup

Austausch eines direkt spezifizierten Elements durch ein anderes, direkt spezifiziertes Element

Innerhalb des Abschnitts **<plan><targets><inclusions>**:

1. Löschen Sie das Tag **<ID>**.
2. Bearbeiten Sie den Wert des Tags **<Path>**, welches die Informationen über die zu sichernden Daten enthält; ersetzen Sie beispielsweise '**C:**' durch '**D:**'.

Austausch eines direkt spezifizierten Elements mit einem Auswahl-Template

Innerhalb des Abschnitts **<plan><options><specific><inclusion_rules>**:

1. Fügen Sie das Tag **<rules_type>** mit dem Wert '**disks**' oder '**files**' hinzu, abhängig vom Typ des von Ihnen benötigten Templates.
2. Fügen Sie das Tag **<rules>** hinzu.
3. Fügen Sie innerhalb des Tags **<rules>** den Eintrag **<rule>** mit dem benötigten Template hinzu. Das Template muss mit dem direkt spezifizierten Element korrespondieren. Falls das spezifizierte Element beispielsweise den Wert '**disks**' hat, dann können Sie die Templates **[SYSTEM]**, **[BOOT]** und **[Fixed Volumes]** verwenden; aber nicht die Templates **[All Files]** oder **[All Profiles Folder]**. Zu weiteren Informationen über Templates siehe 'Auswahlregeln für Volumes (S. 400)' und 'Auswahlregeln für Dateien und Ordner (S. 399)'.
4. Wiederholen Sie Schritt 3, um ein weiteres Template hinzuzufügen.

Beispiel

Das folgende Beispiel illustriert, wie Sie ein direkt spezifiziertes Element mit Auswahl-Templates ersetzen können.

Der ursprüngliche Abschnitt:

```
<specific>
   <backup_type>
      disks
   </backup_type>
   <disk_level_options />
   <file_level_options />
   <inclusion_rules />
<specific>
```

Der Abschnitt nach Anwendung der Auswahl-Templates:

```
<specific>
   <backup_type>
      disks
   </backup_type>
   <disk_level_options />
   <file_level_options />
   <inclusion_rules>
      <rules_type>
         disks
      </rules_type>
      <rules>
         <rule>
            [BOOT]
         </rule>
         <rule>
            [SYSTEM]
         </rule>
      </rules>
   </inclusion_rules>
<specific>
```

14.1.4 Deployment von Backup-Plänen als Dateien

Angenommen, Sie können aus irgendeinem Grund den Acronis Backup & Recovery 11.5 Management Server nicht in Ihrer Umgebung ausführen, aber Sie müssen dennoch ein und denselben Backup-Plan auf mehrere Maschinen anwenden. Eine gute Lösung ist es, den Backup-Plan von einer Maschine zu exportieren und ihn auf alle anderen Maschinen zu verteilen.

Die Funktionsweise

Auf jeder Maschine, auf der ein Agent installiert ist, gibt es einen dedizierten Ordner zum Speichern verteilter Pläne. Der Agent verfolgt Änderungen an diesem dedizierten Ordner. Sobald eine neue .xml-Datei im dedizierten Ordner erscheint, importiert der Agent den entsprechenden Backup-Plan aus dieser Datei. Falls Sie eine .xml-Datei im dedizierten Ordner ändern (oder löschen), ändert (oder löscht) der Agent auch automatisch den dazugehörigen Backup-Plan.

Die Exportdatei bearbeiten

Ein auf solche Art importierter Backup-Plan kann nicht über die grafische Benutzeroberfläche bearbeitet werden. Ein Bearbeiten der Exportdatei (S. 367) ist jedoch vor oder nach dem Deployment per Texteditor möglich.

Falls Sie die Datei vor dem Deployment bearbeiten, dann wirken sich die Änderungen bei allen Maschinen aus, auf die der Plan verteilt wird. Sie können auf Wunsch die direkte Spezifikation des zu sichernden Elementes ändern (beispielsweise C: oder C:\Users) – und zwar per Template (etwa

[SYSTEM] oder [All Profiles Folder]). Zu weiteren Informationen über Templates siehe 'Auswahlregeln für Volumes (S. 400)' und 'Auswahlregeln für Dateien und Ordner (S. 399)'.

Sie können auf Wunsch auch die vom Plan verwendeten Anmeldedaten ändern.

So verteilen Sie einen Backup-Plan als Datei

1. Erstellen Sie auf einer der Maschinen einen Backup-Plan.
2. Exportieren Sie diesen als .xml-Datei (S. 366).
3. [Optional] Bearbeiten Sie die Exportdatei. Zu weiteren Informationen siehe 'Die Exportdatei bearbeiten (S. 367)'.
4. Verteilen Sie diese .xml-Datei zum dedizierten Ordner.

   Der Pfad des dedizierten Ordners

In Windows:

Der Standard-Pfad zum dedizierten Ordner ist **%ALLUSERSPROFILE%\Acronis\BackupAndRecovery\import** (für Windows Vista und späteren Versionen von Windows) oder **%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\import** (für Windows-Versionen vor Windows Vista).

Der Pfad wird im Registry-Schlüssel **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\MMS\Configuration\Import\FolderPath** gespeichert.

Fehlt der Schlüssel, so bedeutet das, dass der Agent den dedizierten Ordner nicht überwacht.

Bearbeiten Sie diesen Schlüssel, um den Pfad zu ändern. Die Änderung wird erst nach einem Neustart des **Acronis Managed Machine Service** übernommen.

In Linux:

Der Standard-Pfad zum dedizierten Ordner ist **/usr/lib/Acronis/BackupAndRecovery/import**.

Der Pfad wird in der Datei **/etc/Acronis/MMS.config** gespeichert.

Bearbeiten Sie zur Änderung des Pfades den Wert **`/usr/lib/Acronis/BackupAndRecovery/import`** in folgendem Tag:

```
<key name="Import">
        <value name="FolderPath" type="TString">
               "/usr/lib/Acronis/BackupAndRecovery/import"
        </value>
</key>
```

Die Änderung wird erst nach einem Neustart des Agenten übernommen. Führen Sie folgenden Befehl als Benutzer 'root' aus, um den Agenten neu zu starten:

```
/etc/init.d/acronis_mms restart
```

Fehlt der Tag, so bedeutet das, dass der Agent den dedizierten Ordner nicht überwacht.

14.1.5 Backup-Plan-Details

Das Fenster **Backup-Plan-Details** (auch noch mal im Fensterbereich **Informationen** verfügbar) fasst alle Informationen zu einem ausgewählten Backup-Plan zusammen.

Falls die Ausführung des Plans einen Benutzereingriff erfordert, erscheint im oberen Bereich der Registerlaschen eine entsprechende Meldung. Die Nachricht enthält eine kurze Beschreibung des

Problems und Aktionsschaltflächen, über die Sie die passende Aktion wählen oder den Plan stoppen können.

Details

Die Registerlasche **Backup-Pläne und Tasks** stellt folgende allgemeine Informationen über einen ausgewählten Plan zur Verfügung:

- **Name** – Bezeichnung des Backup-Plans
- **Ursprung** – ob der Plan direkt auf der Maschine erstellt wurde (lokaler Ursprung) oder vom Management Server auf der Maschine bereitgestellt wurde (zentraler Ursprung).
- **Ausführungsstadium** – Ausführungsstadium (S. 363) des Backup-Plans.
- **Status** – Status (S. 364) des Backup-Plans.
- **Maschine** – Name der Maschine, auf der der Backup-Plan existiert (nur für zentrale Backup-Pläne).
- **Planung** – ob der Task über eine Zeit-/Ereignisplanung verfügt oder auf manuellen Start gesetzt ist.
- **Letzte Startzeit** – wie viel Zeit seit dem letzten Plan- oder Task-Start verstrichen ist.
- **Deployment-Stadium** – die Deployment-Stadien des Backup-Plans (nur für zentrale Backup-Pläne).
- **Letzte Abschlusszeit** – wie viel Zeit seit der letzten Plan- oder Task-Fertigstellung verstrichen ist.
- **Letztes Ergebnis** – das Ergebnis der letzten Plan- oder Task-Ausführung.
- **Typ** – Typ des Backup-Plans oder Tasks.
- **Besitzer** – Name des Benutzers, der den Plan erstellt oder zuletzt modifiziert hat.
- **Nächste Startzeit** – wann der Plan oder Task das nächste Mal gestartet wird.
- **Kommentar** – Beschreibung des Plans (sofern verfügbar).

Tasks

In der Registerlasche **Tasks** wird eine Liste aller Tasks des gewählten Backup-Plans angezeigt. Klicken Sie auf **Details**, um sich Details zum gewählten Task anzeigen zu lassen.

Fortschritt

In der Registerlasche **Fortschritt** werden alle Aktivitäten eines gewählten Backup-Plans aufgelistet, die gerade ablaufen oder auf ihre Ausführung warten.

Verlauf

In der Registerlasche **Verlauf** können Sie den Verlauf aller vom Backup-Plan ausgeführten Aktivitäten untersuchen.

Backup-Quelle

Die Registerlasche **Quelle** stellt die folgenden Informationen über die zum Backup ausgewählten Daten zur Verfügung:

- **Quelltyp** – die Art der Daten, die zum Backup ausgewählt wurden
- **Elemente für das Backup** – die für die Sicherung ausgewählten Elemente und ihre Größe

Backup-Ziel

Die Registerlasche **Ziel** stellt die folgenden Informationen zur Verfügung:

- **Name** – Name des Archivs.
- **Speicherort** – Bezeichnung des Depots oder Pfad zu dem Verzeichnis, wo das Archiv gespeichert wird
- **Archiv-Kommentare** – Beschreibung zu einem Archiv (sofern vorhanden)
- **2.**, **3.**, **4.**, **5. Speicherort** – Namen der Speicherorte, zu denen das Archiv kopiert oder verschoben wurde (falls im Backup-Plan entsprechend konfiguriert).

Einstellungen

Die Registerlasche **Einstellungen** zeigt die folgenden Informationen:

- **Backup-Schema** – das gewählte Backup-Schema und all seine Einstellungen inkl. Planung
- **Validierung** – falls spezifiziert, Ereignisse vor oder nach Ausführung einer Validierung bzw. einer Validierungsplanung. Falls keine Validierung eingestellt wurde, wird der Wert **Nie** angezeigt.
- **Backup-Optionen** – gegenüber den Standardwerten veränderte Backup-Optionen

14.1.6 Task-/Aktivitätsdetails

Das Fenster **Task-/Aktivitätsdetails** (wird auch im Fensterbereich **Informationen** dupliziert) sammelt auf mehreren Registerlaschen alle Informationen über einen gewählten Task bzw. eine Aktivität.

Wenn ein Task oder eine Aktivität einen Benutzereingriff erfordert, dann erscheinen eine Meldung und Aktionsschaltflächen über den Registerlaschen. Die Meldung enthält eine kurze Beschreibung des Problems. Die Schaltflächen ermöglichen, den Task oder die Aktivität zu wiederholen oder zu stoppen.

14.2 Log

Das lokale Ereignis-Log speichert den Verlauf aller von Acronis Backup & Recovery 11.5 auf der Maschine durchgeführten Aktionen.

Wählen Sie zur Anzeige einer einfachen Liste von Log-Einträgen das Element **Ereignisse** aus dem Listenfeld **Anzeige** – um nach Aktivitäten gruppierte Log-Einträge angezeigt zu bekommen, wählen Sie **Aktivitäten**. Details zu einem ausgewählten Log-Eintrag oder einer Aktivität werden im Fensterbereich **Informationen** angezeigt (im unteren Teil der **Log**-Anzeige).

Verwenden Sie Filter, um gewünschte Aktivitäten und Log-Einträge in der Tabelle anzeigen zu lassen. Sie können außerdem nicht benötigte Spalten ausblenden bzw. ausgeblendete wieder aktivieren. Zu Details siehe 'Tabellenelemente sortieren, filtern und konfigurieren (S. 29)'.

Wählen Sie eine Aktivität oder Log-Eintrag aus, um auf diese eine Aktion ausführen zu lassen. Zu Details siehe 'Aktionen für Log-Einträge (S. 372)' und 'Details zu Log-Einträgen (S. 373)'.

14.2.1 Aktionen für Log-Einträge

Alle nachfolgend beschriebenen Aktionen werden durch Klicken auf die korrespondierenden Elemente in der Log-**Symbolleiste** ausgeführt. Diese Aktionen können außerdem über das Kontextmenü durchgeführt werden (indem Sie mit der rechten Maustaste auf den Log-Eintrag oder die Aktivität klicken).

Nachfolgend finden Sie eine Anleitung zur Ausführung von Aktionen auf Log-Einträge.

Aufgabe	Lösung
Eine einzelne Aktivität wählen	Wählen Sie **Aktivitäten** aus dem Listenfeld **Anzeige** und klicken Sie dann auf die gewünschte Aktivität. Im Fensterbereich **Informationen** werden für die gewählte Aktivität die Log-Einträge angezeigt.
Einen einzelnen Log-Eintrag wählen	Klicken Sie auf ihn.
Mehrere Log-Einträge wählen	▪ *Nicht zusammenhängend*: Halten Sie **Strg** gedrückt und klicken Sie nacheinander auf die gewünschten Log-Einträge ▪ *Zusammenhängend*: wählen Sie einen einzelnen Log-Eintrag, halten Sie dann die **Umschalt**-Taste gedrückt und klicken Sie auf einen weiteren Log-Eintrag. Darauf werden auch alle Log-Einträge zwischen der ersten und letzten Markierung ausgewählt.
Details zu einem Log-Eintrag einsehen	1. Wählen Sie einen Log-Eintrag. 2. Wählen Sie eine der nachfolgenden Varianten: ▪ Klicken Sie doppelt auf die Auswahl. ▪ Klicken Sie auf **Details**. Die Details des Log-Eintrags werden angezeigt. Zu Details über Aktionen für Log-Einträge siehe den Abschnitt 'Details zu Log-Einträgen (S. 437)'.
Gewählte Log-Einträge in eine Datei speichern	1. Lassen Sie die **Aktivitäten** anzeigen und wählen Sie die entsprechenden Aktivitäten oder lassen Sie die **Ereignisse** anzeigen und wählen Sie die entsprechenden Log-Einträge. 2. Klicken Sie auf **Auswahl in Datei speichern**. 3. Vergeben Sie im geöffneten Fenster einen Pfad und Namen für die Datei. Alle Log-Einträge der gewählten Aktivitäten oder gewählten Log-Einträge werden in eine spezifizierte Datei gespeichert.
Alle Log-Einträge in eine Datei speichern	1. Stellen Sie sicher, dass keine Filter gesetzt sind. 2. Klicken Sie auf **Alle in Datei speichern**. 3. Vergeben Sie im geöffneten Fenster einen Pfad und Namen für die Datei. Alle Log-Einträge werden in die spezifizierte Datei gespeichert.
Alle gefilterten Log-Einträge in eine Datei speichern	1. Setzen Sie Filter, um eine Liste von Log-Einträgen zu erhalten, die den Filterkriterien entsprechen. 2. Klicken Sie auf **Alle in Datei speichern**. 3. Vergeben Sie im geöffneten Fenster einen Pfad und Namen für die Datei. Alle Log-Einträge in der Liste werden in die spezifizierte Datei gespeichert.
Alle Log-Einträge löschen	Klicken Sie auf **Alle Löschen**. Alle Einträge werden aus dem Log gelöscht und es wird ein neuer Log-Eintrag erstellt. Er enthält Informationen darüber, wer die Log-Einträge gelöscht hat und wann.

14.2.2 Details zu Log-Einträgen

Zeigt für den gewählten Log-Eintrag detaillierte Informationen an und erlaubt Ihnen, die Details in die Zwischenablage zu kopieren.

Um Details des nächsten oder vorherigen Log-Eintrages einsehen zu können, müssen Sie auf die Schaltfläche mit dem Pfeil nach unten bzw. oben klicken.

Klicken Sie auf die Schaltfläche **In Zwischenablage kopieren**, um die Details zu kopieren.

Datenfelder der Log-Einträge

Ein Log-Eintrag enthält folgende Datenfelder:

- **Typ** – Ereignistyp (Fehler, Warnung, Information).
- **Datum und Zeit** – Datum und Uhrzeit, wann das Ereignis stattfand.
- **Backup-Plan** – der Backup-Plan, auf den sich das Ereignis bezieht (sofern vorhanden).
- **Task** – Der Task, auf den sich das Ereignis bezieht (sofern vorhanden).
- **Code** – Kann leer sein oder dem Programmfehlercode entsprechen, wenn das Ereignis vom Typ „Fehler" ist. Der Fehlercode ist eine Integer-Zahl, die vom Acronis-Support zum Lösen des Problems verwendet werden kann.
- **Modul** – Kann leer sein oder der Nummer des Programmmoduls entsprechen, bei dem das Ereignis aufgetreten ist. Es handelt sich um eine Integer-Zahl, die vom Acronis Support Service verwendet werden kann, um das Problem zu lösen.
- **Besitzer** – Der Benutzername des Backup-Plan-Besitzers (S. 35).
- **Nachricht** – Eine Textbeschreibung des Ereignisses.

Die Anzeige von Datum und Zeit variiert in Abhängigkeit von Ihren lokalen Einstellungen.

14.3 Alarmmeldungen

Ein Alarm ist eine Nachricht, die vor gegenwärtigen oder potentiellen Problemen warnt. In der Ansicht **Alarmmeldungen** können Sie die Probleme schnell identifizieren und lösen, indem Sie die aktuellen Alarmmeldungen überwachen und den Alarmverlauf einsehen.

Aktive und inaktive Alarmmeldungen

Ein Alarm kann sich entweder in einem aktiven oder inaktiven Stadium befinden. Ein aktives Stadium bedeutet, dass das Problem, welches den Alarm verursacht hat, immer noch existiert. Ein aktiver Alarm wird inaktiv, wenn das Problem, das den Alarm verursacht hat, entweder manuell oder von alleine gelöst wurde.

***Anmerkung**: Es gibt einen Alarmtyp, der immer aktiv ist: „Backup nicht erstellt". Hintergrund ist, dass selbst bei erfolgreicher Behebung der Alarmursache und erfolgreicher Erstellung anderer, nachfolgender Backups, die Tatsache immer noch bestehen bleibt, dass das Backup nicht erstellt wurde.*

Probleme beheben, die Alarmmeldungen verursacht haben

Klicken Sie auf **Problem beheben**, um die Alarmursache herauszufinden und zu beseitigen. Sie werden daraufhin zur entsprechenden Ansicht geführt,wo Sie das Problem untersuchen und die notwendigen Schritte zu seiner Lösung durchführen können.

Sie können optional auch auf **Details anzeigen** klicken, um mehr Informationen über den von Ihnen gewählten Alarm zu erhalten.

Alarmmeldungen annehmen

Standardmäßig listet die Tabelle **Aktuelle Alarmmeldungen** sowohl aktive als auch inaktive Alarmmeldungen auf, solange bis diese nicht mehr akzeptiert werden. Um einen Alarm anzunehmen, wählen Sie diesen aus und klicken dann auf den Befehl **Annehmen**. Indem Sie einen Alarm

annehmen, nehmen Sie ihn zur Kenntnis und übernehmen dieVerantwortung für ihn. Die angenommenen Alarmmeldungen werden dann ohne Änderung ihres Alarmstadiums zur Tabelle **Angenommene Alarmmeldungen** verschoben.

Die Tabelle **Angenommene Alarmmeldungen** speichert so einen Verlauf aller angenommenen Alarmmeldungen. Sie können hier herausfinden, wer einen Alarm angenommen hat und wann sich dieser ereignete. Angenommene Alarmmeldungen beider Stadien können aus der Tabelle entweder manuell entfernt werden – durch Verwendung der Schaltflächen **Löschen** und **Alle löschen** – oder automatisch entfernt werden (siehe „Alarmmeldungen konfigurieren“ weiter unten in diesem Abschnitt).

Indem Sie auf **Alle in Datei speichern** klicken, können Sie den kompletten Tabelleninhalt in eine *.txt- oder *.csv-Datei exportieren.

Alarmmeldungen konfigurieren

Verwenden Sie zur Konfiguration von Alarmmeldungen folgende Optionen aus dem oberen Bereich der Anzeige **Alarmmeldungen**.

- **Alarmmeldungen anzeigen/verbergen** (S. 31) – spezifizieren Sie den Alarmtyp, der in der Ansicht **Alarmmeldungen** angezeigt werden soll.
- **Benachrichtigungen** (S. 380) – konfigurieren Sie die E-Mail-Benachrichtigungen über Alarmmeldungen.
- **Einstellungen** (S. 378) – spezifizieren Sie, ob inaktive Alarmmeldungen automatisch in die Tabelle **Angenommene Alarmmeldungen** verschoben werden sollen; konfigurieren Sie, wie lange die angenommenen Alarmmeldungen in der Tabelle **Angenommene Alarmmeldungen** bewahrt werden sollen.

14.4 Eine Lizenz wechseln

Bei einem Lizenzwechsel wechseln Sie zu einer anderen Version oder Edition des Produkts. Die nachfolgende Tabelle fasst die verfügbaren Optionen zusammen.

Eine Lizenz wechseln	Warum er erforderlich sein kann
Testlizenz –> Vollversion	Sie haben nach dem Testen des Produktes eine Lizenz gekauft.
Vollversion –> Vollversion, andere Edition	▪ Sie möchten ein Upgrade von Acronis Backup & Recovery 11.5 durchführen – und zwar von einem Standalone-Produkt zur Advanced-Plattform aktualisieren, um die Möglichkeit zur zentralen Verwaltung zu nutzen. Weitere Informationen finden Sie im Abschnitt 'Upgrade von einem Standalone-Produkt zur Advanced-Plattform' der Installationsanleitung. ▪ Sie haben die Lizenz einer Server-Edition für eine Workstation verwendet. Sie wollen jetzt der Workstation eine Workstation-Lizenz zuweisen. Sie können danach die für den Server widerrufen und Sie für einen anderen Server verwenden. ▪ Eine Maschine hat eine Advanced Server-Lizenz, welche Ihnen ermöglicht, 4 virtuelle Maschinen zu sichern. Um mehr virtuelle Maschinen sichern zu können, müssen Sie der Maschine die Lizenz für eine Virtual-Edition zuweisen.
Vollversion –> Vollversion + Add-on	Sie haben eine Add-on-Lizenz erworben, beispielsweise 'Universal Restore' oder 'Deduplication'.

Backups zum Online Storage* –> Vollversion	Sie haben nach der Erstellung von Backups zum Online Storage entschieden, dass Sie eine Edition mit mehr Funktionalität testen oder erwerben wollen.
Testversion –> Backups zum Online Storage*	Sie haben nach dem Test des Produktes entschieden, dass Sie nur Backups zum Online Storage durchführen wollen.

*Online Backups stehen für Maschinen, die unter Linux laufen, nicht zur Verfügung. Bestimmte Datentypen (etwa Exchange-Datenbanken) können nicht zum Online Storage gesichert werden. Bevor Sie Ihre Backups auf dem Online Storage sichern können, müssen Sie auf den Maschinen, die Sie sichern wollen, ein Abonnement für den Online Backup Service aktivieren. Weitere Informationen finden Sie im Abschnitt 'Online Backup (S. 460)'.

Vor dem Umstellen vom Testmodus zur Vollversion

Falls Sie vorhaben, die Lizenzen auf einer großen Zahl von Maschinen zu wechseln, können Sie die Lizenzschlüssel dem Acronis License Server hinzufügen (in diesen importieren).

Acronis Deduplication ist in der Testversion immer aktiviert. Wenn Sie diese Funktion weiterhin benutzen wollen, denken Sie daran:

1. Lizenzen für Acronis Deduplication zu erwerben.
2. Die Lizenzschlüssel für Acronis Deduplication in den License Server zu importieren (empfohlen).
3. Verwenden Sie eine Acronis Deduplication-Lizenz für jede Maschine, auf der Acronis Backup & Recovery 11.5 auf die Vollversion umgestellt wird.

Dies ist auch zu einem späteren Zeitpunkt möglich; allerdings werden bis dahin alle Backups zu deduplizierenden Depots fehlschlagen.

Zugriff auf das Fenster 'Lizenzen'

Wählen Sie aus den nachfolgenden Varianten:

- Verbinden Sie, um die Lizenz einer verwalteten Maschine zu ändern, die Konsole mit der Maschine und klicken Sie dann auf **Hilfe** –> **Lizenz wechseln**.
- Vverbinden Sie, um die Lizenz einer verwalteten Maschine zu ändern, die Konsole mit dem Management Server, navigieren Sie zu **Maschinen mit Agenten** –> **Alle Maschinen mit Agenten** – oder navigieren Sie zu einer anderen Gruppe, welche die Maschinen anzeigt, deren Lizenz Sie wechseln wollen. Klicken Sie dann mit der rechten Maustaste auf die Maschine und anschließend auf **Lizenz wechseln**.
- Verbinden Sie, um die Lizenz eines Virtualisierungshosts zu wechseln (ausgenommen bei einem geclusterten Host), die Konsole mit dem Management Server, navigieren Sie zu **Virtuelle Maschinen** –> **Hosts und Cluster**, klicken Sie mit der rechten Maustaste auf den Host und dann auf den Befehl **Lizenz wechseln**.
- Verbinden Sie, um die Lizenzen aller Hosts eines Virtualisierungsclusters zu wechseln, die Konsole mit dem Management Server, navigieren Sie zu **Virtuelle Maschinen** –> **Hosts und Cluster**, klicken Sie mit der rechten Maustaste auf den Cluster und dann auf den Befehl **Lizenz wechseln**.

Eine Lizenz wechseln

Sie können im Fenster **Lizenzen** Lizenzschlüssel hinzufügen und auswählen, welche Lizenzen für eine ausgewählte Maschine verwendet werden soll. Jede Lizenz ermöglicht einen bestimmten Satz an Funktionen. Falls Sie sich dazu entscheiden, keine Lizenz zu verwenden, können Sie nur Backups zum Online Storage durchführen.

Sie können in diesem Fenster außerdem den License Server ändern, der von der Maschine verwendet wird. Diese Aktion ist nur möglich, sofern die Maschine nicht auf dem Management Server registriert ist. Bei registrierten Maschinen bestimmt der Management Server, welchen License Server die Maschinen verwenden. Weitere Details finden Sie im Abschnitt 'Den vom Management Server verwendeten License Server ändern (S. 427)'.

Ein Online Backup-Abonnement verwalten

Der Block **Acronis Cloud** im Fenster **Lizenzen** erfordert es, dass Sie sich an Ihrem Acronis-Konto anmelden. Danach zeigt er das auf der Maschine aktivierte Online Backup-Abonnement an. Sollte kein Abonnement aktiviert sein, dann ermöglicht Ihnen dieser Block, ein Abonnement anzufordern, den nach dem Abonnementkauf erhaltenen Registrierungscode einzugeben und das Abonnement zu aktivieren.

14.5 Sammeln von Systeminformationen

Das Werkzeug zum Sammeln von Systeminformationen trägt Daten über die Maschine zusammen, mit der die Management Konsole verbunden ist, und speichert sie in einer Datei. Wenn Sie den technischen Support von Acronis kontaktieren, können Sie ihm diese Datei zur Verfügung stellen.

Diese Option ist bei bootfähigen Medien verfügbar und für Maschinen, auf denen der Agent für Windows, Agent für Linux, oder der Acronis Backup & Recovery 11.5 Management Server installiert ist.

So sammeln Sie Systeminformationen

1. Wählen Sie in der Management Konsole aus dem Hauptmenü **Hilfe** –> **Systeminformation von 'Maschinenname' sammeln**.
2. Spezifizieren Sie einen Speicherort für die Datei mit den Systeminformationen.

14.6 Die Maschinen-Optionen anpassen

Die Maschinen-Optionen definieren das allgemeine Verhalten von allen Acronis Backup & Recovery 11.5-Agenten, die auf der verwalteten Maschine operieren und werden daher als spezifisch für die Maschine betrachtet.

Um auf die Maschinen-Optionen zuzugreifen, verbinden Sie die Konsole zur verwalteten Maschine und wählen dann im Menü **Optionen –> Maschinen-Optionen**.

14.6.1 Erweiterte Einstellungen

Spezifizieren Sie, was geschehen soll, wenn die Maschine bei einer Task-Ausführung heruntergefahren werden soll.

Diese Option ist nur für Windows-Betriebssysteme wirksam.

Sie bestimmt das Verhalten von Acronis Backup & Recovery 11.5, wenn das System herunterfährt. Dieses System-Herunterfahren tritt auf, wenn die Maschine ausgeschaltet oder neu gestartet wird.

Voreinstellung ist: **Laufende Tasks stoppen und herunterfahren.**

Falls Sie die Option **Laufende Tasks stoppen und herunterfahren** aktivieren, werden alle laufenden Tasks von Acronis Backup & Recovery 11.5 abgebrochen.

Falls Sie die Option **Auf Task-Abschluss warten** wählen, werden alle laufenden Tasks von Acronis Backup & Recovery 11.5 noch fertiggestellt.

14.6.2 Acronis Programm zur Kundenzufriedenheit (CEP)

Diese Option ist nur für Windows-Betriebssysteme wirksam.

Diese Option legt fest, ob die Maschine am Acronis Programm zur Kundenzufriedenheit (CEP) teilnimmt.

Falls Sie **Ja, ich möchte am CEP teilnehmen** aktivieren, werden auf der Maschine Informationen gesammelt (über die Hardware-Konfiguration, am häufigsten und am wenigsten verwendete Funktionen, sowie Probleme) und regelmäßig an Acronis geschickt. Die Ergebnisse sind dazu gedacht, Verbesserungen bei der Software und Funktionalität zu ermöglichen, um die Bedürfnisse von Acronis-Kunden noch besser zu erfüllen.

Acronis sammelt keine persönliche Daten. Lesen Sie die Teilnahmebedingungen auf der Acronis-Website oder in der Benutzeroberfläche des Produkts, um mehr über das CEP zu erfahren.

Die Option wird anfangs während der Installation des Acronis Backup & Recovery 11.5-Agenten konfiguriert. Sie können diese Einstellung jederzeit in der Benutzeroberfläche des Programms ändern (**Optionen** –> **Maschinen-Optionen** –> **Programm zur Kundenzufriedenheit (CEP)**). Diese Option kann außerdem durch Verwendung der Gruppenrichtlinien-Infrastruktur (S. 445) konfiguriert werden. Eine per Gruppenrichtlinie definierte Einstellung kann nicht durch Verwendung der Programmoberfläche geändert werden, außer die Gruppenrichtlinie wird auf der Maschine deaktiviert.

14.6.3 Alarmmeldungen

14.6.3.1 Alarmverwaltung

Elemente von „Angenommene Alarmmeldungen“ entfernen, wenn älter als

Diese Option definiert, ob Meldungen aus der Tabelle für **Angenommene Alarmmeldungen** gelöscht werden sollen.

Voreinstellung ist: **Deaktiviert**.

Wenn aktiviert, können Sie für die angenommenen Alarmmeldungen einen Aufbewahrungszeitraum spezifizieren. Angenommene Alarmmeldungen, die älter als dieser Zeitraum sind, werden automatisch aus der Tabelle gelöscht.

Inaktive Alarmmeldungen automatisch zu „Angenommene Alarmmeldungen“ verschieben

Diese Option definiert, ob alle Alarmmeldungen, die inaktiv werden, angenommen und automatisch in die Tabelle **Angenommene Alarmmeldungen** verschoben werden sollen.

Voreinstellung ist: **Deaktiviert**.

Wenn aktiviert, können Sie die Alarmtypen spezifizieren, auf die diese Option angewendet wird.

14.6.3.2 Zeit-basierte Alarmmeldungen

Letztes Backup

Diese Option ist wirksam, wenn die Konsole mit einer verwalteten Maschine (S. 496) oder zum Management Server (S. 493) verbunden ist.

Die Option legt fest, ob eine Warnung erscheint, wenn auf der gegebenen Maschine nach Ablauf einer Zeitspanne kein Backup durchgeführt wurde. Sie können den Zeitraum einrichten, den Sie als kritisch für Ihr Geschäftsumfeld betrachten.

Voreinstellung ist: Warnen, wenn die letzte erfolgreiche Sicherung auf einer Maschine vor mehr als **5 Tagen** abgeschlossen wurde.

Der Alarm wird in der Ansicht **Alarmmeldungen** des Fensterbereichs **Navigation** angezeigt. Wenn die Konsole mit dem Management Server verbunden ist, wird diese Einstellung auch das Farbschema der Spalte **Letztes Backup** für jede Maschine steuern.

Letzte Verbindung

Diese Option ist wirksam, wenn die Konsole mit einer registrierten Maschine (S. 494) oder zum Management Server verbunden ist.

Die Option legt fest, ob eine Warnung erscheint, wenn innerhalb einer eingerichteten Zeitspanne keine Verbindung zwischen einer registrierten Maschine und dem Management Server hergestellt wurde, die Maschine also möglicherweise nicht zentral verwaltet wurde (z.B. bei einem Ausfall der Netzverbindung zu dieser Maschine). Sie können die Zeitspanne festlegen, die als kritisch erachtet wird.

Voreinstellung ist: Warnen, wenn die letzte Verbindung der Maschine zum Management Server vor mehr als **5 Tagen** war.

Der Alarm wird in der Ansicht **Alarmmeldungen** des Fensterbereichs **Navigation** angezeigt. Wenn die Konsole mit dem Management Server verbunden ist, wird diese Einstellung auch das Farbschema der Spalte **Letzte Verbindung** für jede Maschine steuern.

14.6.4 E-Mail-Einstellungen

Diese Option ermöglicht Ihnen E-Mail-Einstellungen zu konfigurieren, um Benachrichtigungen über Alarmmeldungen, die auf der verwalteten Maschine aufgetreten sind, zu versenden.

Die Benachrichtigungsplanungen und Arten der zu versendenden Alarmmeldungen werden unter **Maschinen-Optionen** –> **E-Mail-Einstellungen** –> **Alarmbenachrichtigungen** (S. 380) konfiguriert.

Voreinstellung ist: **Deaktiviert**.

Hinweis: *Alarmmeldungen warnen nur über Probleme. E-Mail-Benachrichtigungen über erfolgreiche Backup- und Recovery-Aktionen werden daher nicht versendet. Diese E-Mail-Benachrichtigungen werden unter Backup-Optionen –> Benachrichtigungen –> E-Mail (S. 131) bzw. unter Recovery-Optionen –> Benachrichtigungen –> E-Mail (S. 185) konfiguriert.*

So konfigurieren Sie eine E-Mail-Benachrichtigung

1. Geben Sie die E-Mail-Adresse des Ziels im Feld **E-Mail-Adressen** ein. Sie können auch mehrere, per Semikolon getrennte Adressen eingeben.
2. Geben Sie in das Feld **Betreff** eine Beschreibung der Benachrichtigung ein oder lassen Sie den Wert leer. In dem Feld werden keine Variablen unterstützt.

3. Geben Sie im Feld **SMTP-Server** den Namen des ausgehenden Mail-Servers (SMTP) ein.
4. Legen Sie im Feld **Port** die Port-Nummer des ausgehenden Mail-Servers fest. Standardmäßig ist der Port auf **25** gesetzt.
5. Sollte der ausgehende Mail-Server eine Authentifizierung benötigen, dann geben Sie den **Benutzernamen** und das **Kennwort** vom E-Mail-Konto des Senders ein.

   Sollte der SMTP-Server keine Authentifizierung benötigen, dann lassen Sie die Felder **Benutzername** und **Kennwort** einfach leer. Falls Sie nicht sicher sind, ob Ihr SMTP-Server eine Authentifizierung erfordert, dann kontaktieren Sie Ihren Netzwerk-Administrator oder bitten Sie Ihren E-Mail-Dienstanbieter um Hilfe.
6. Klicken Sie auf **Erweiterte E-Mail-Parameter...**, um weitere E-Mail-Parameter folgendermaßen zu konfigurieren:
   a. **Von** – geben Sie den Namen des Absenders an. Falls Sie das Feld leer lassen, dann enthalten die Nachrichten im Feld **Von** das E-Mail-Konto des Senders.
   b. **Verschlüsselung verwenden** – Sie können sich für eine verschlüsselte Verbindung zum Mail-Server entscheiden. Zur Auswahl stehen die Verschlüsselungstypen SSL und TLS.
   c. Einige Internetdienstanbieter verlangen eine Authentifizierung am Posteingangsserver, bevor das Verschicken von Nachrichten erlaubt wird. Wenn das bei Ihnen zutrifft, aktivieren Sie das Kontrollkästchen **Anmeldung beim Posteingangsserver**, um einen POP3-Server zu aktivieren und seine Einstellungen einzurichten:
      - **Posteingangsserver (POP3)** – geben Sie den Namen des POP3-Servers an.
      - **Port** – bestimmt den Port des POP3-Servers. Standardmäßig ist der Port auf **110** gesetzt.
      - **Benutzername** und **Kennwort** für den eingehenden Mail-Server.
   d. Klicken Sie auf **OK**.
7. Klicken Sie auf **Test-Mail senden**, um zu überprüfen, ob die E-Mail-Benachrichtigungen mit den spezifizierten Einstellungen korrekt funktionieren.

14.6.4.1 Alarmbenachrichtigungen

Diese Option ermöglicht Ihnen festzulegen, wann E-Mail-Benachrichtigungen über Alarmmeldungen, die auf der verwalteten Maschine aufgetreten sind, versendet werden sollen – und zudem festzulegen, welche Arten von Alarmmeldungen versendet werden sollen.

Stellen Sie bei Verwendung dieser Option sicher, dass die E-Mail-Benachrichtigungen unter **Maschinen-Optionen** –> **E-Mail-Einstellungen** (S. 379) korrekt konfiguriert sind.

Voreinstellung ist: **Deaktiviert**.

So konfigurieren Sie die Alarmbenachrichtigungen

1. Wählen Sie, wann die Alarmbenachrichtigungen versendet werden sollen:
   - **Sobald ein Alarm auftritt** – um eine Benachrichtigung jedes Mal zu versenden, wenn ein neuer Alarm auftritt.

     Klicken Sie auf **Wählen Sie den Typ der Alarmmeldungen...**, um festzulegen, bei welcher Art von Alarm Benachrichtigungen versendet werden sollen.
   - **Benachrichtigung über alle aktuellen Alarmmeldungen nach Plan senden** – um eine gesammelte Alarmbenachrichtigung zu versenden, die alle Alarmmeldungen enthält, die in einer von Ihnen spezifizierten Zeitspanne aufgetreten sind.

     Klicken Sie auf **Wählen Sie den Typ der Alarmmeldungen...**, um festzulegen, bei welcher Art von Alarm Benachrichtigungen versendet werden sollen.

     Konfigurieren Sie die **Frequenz** und **Zeit** der Benachrichtigung.

2. Klicken Sie auf **OK**.

14.6.5 Ereignisverfolgung

Es ist möglich, die von auf der verwalteten Maschine agierenden Agenten erstellten Logs in die Ereignisanzeige von Windows zu duplizieren oder an spezifizierte SNMP-Manager zu senden. Wenn Sie die Optionen zur Ereignisverfolgung an keiner anderen Stelle außer dieser verändern, werden die Einstellungen für jeden lokalen Backup-Plan und jeden erstellten Task auf der Maschine wirksam.

Sie können die Einstellungen in den Standardoptionen fьr Backup und Recovery exklusiv für die Ereignisse überschreiben, die während eines Backups oder einer Wiederherstellung auftreten. In diesem Fall werden die hier vorgenommenen Einstellungen auch wirksam für andere Tasks, z.B. für die Validierung von Archiven oder die Bereinigung.

Sie können die als Standard gesetzten Optionen auch überschreiben, wenn Sie einen Backup-Plan oder einen Recovery-Task einrichten. Diese so vorgenommenen Einstellungen werden plan-spezifisch oder task-spezifisch verwendet.

14.6.5.1 SNMP-Benachrichtigungen

Diese Option ist für Windows und Linux-Betriebssysteme wirksam.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Diese Option definiert, ob Agenten auf verwalteten Maschinen Log-Ereignisse zu spezifizierten Simple Network Management Protocol (SNMP)-Managern schicken. Sie können die Arten der Ereignisse wählen, die geschickt werden.

Sie können die Einstellungen in den Standardoptionen fьr Backup und Recovery exklusiv für die Ereignisse überschreiben, die während eines Backups oder einer Wiederherstellung auftreten. In diesem Fall werden die hier vorgenommenen Einstellungen auch wirksam für andere Tasks, z.B. für die Validierung von Archiven oder die Bereinigung.

Sie können die als Standard gesetzten Optionen auch überschreiben, wenn Sie einen Backup-Plan oder einen Recovery-Task einrichten. Diese so vorgenommenen Einstellungen werden plan-spezifisch oder task-spezifisch verwendet.

Zu weiteren Informationen über die Verwendung von SNMP mit Acronis Backup & Recovery 11.5 siehe „Unterstьtzung fьr SNMP (S. 56)“.

Voreinstellung ist: **Ausgeschaltet**.

Versenden von SNMP-Benachrichtigungen einrichten

1. Aktivieren Sie das Kontrollkästchen **Meldungen an den SNMP-Server schicken**.
2. Spezifizieren Sie die passenden Optionen wie folgt:
   - **Ereignisse, die übermittelt werden** – Auswahl der Ereignistypen, die gesendet werden: **Alle Ereignisse**, **Fehler und Warnungen** oder **Nur Fehler**.
   - **Server-Name/IP** – Eintragen des Namens oder der IP-Adresse des Hosts mit der SNMP-Verwaltungsanwendung, an die die Meldungen gesendet werden.
   - **Community** – Eintragen des Namens der SNMP-Community, zu der der Host mit der SNMP-Verwaltungsanwendung und die sendende Maschine gehören. Die typische Community ist „public“.

   Klicken Sie auf **Testnachricht senden**, um die Richtigkeit der Einstellungen zu prüfen.

Um die Funktion auszuschalten, deaktivieren Sie das Kontrollkästchen **Meldungen an den SNMP-Server schicken**.

Die Nachrichten werden über UDP verschickt.

Der nächste Abschnitt enthält zusätzliche Informationen über das Einstellen der SNMP-Dienste auf den empfangenden Maschinen (S. 382).

14.6.5.2 Einstellen der SNMP-Dienste auf der empfangenden Maschine

Windows

So installieren Sie den SNMP-Dienst auf einer Windows-Maschine:

1. **Start -> Systemsteuerung -> Software -> Windows-Komponenten hinzufügen/entfernen**
2. Wählen Sie **Verwaltungs- und Überwachungsprogramme.**
3. Klicken Sie auf **Details**.
4. Aktivieren Sie das Kontrollkästchen bei **SNMP (Simple Network Management Protocol)**.
5. Klicken Sie auf **OK**.

Sie sollten dann nach der Datei lmmib2.dll gefragt werden, die sich auf dem Installationsmedium des Betriebssystems befindet.

Linux

Um SNMP-Nachrichten auf einer Linux-Maschine zu empfangen, muss das Paket net-snmp (für RHEL und SUSE) oder das Paket snmpd (für Debian) installiert werden.

SNMP kann mit dem Befehl **snmpconf** konfiguriert werden. Die Standardkonfigurationsdateien befinden sich im Verzeichnis /usw/snmp:

- /etc/snmp/snmpd.conf – Konfigurationsdatei für den Net-SNMP Agenten
- /etc/snmp/snmpd.conf – Konfigurationsdatei für den Net-SNMP Trap Daemon.

14.6.5.3 Ereignisanzeige von Windows

Diese Option ist nur wirksam in Windows-Betriebssystemen.

Diese Option ist nicht verfügbar beim Arbeiten nach dem Start vom Boot-Medium.

Diese Option definiert, ob Agenten auf verwalteten Maschinen die Ereignisse in der Ereignisanzeige von Windows aufzeichnen müssen. (Um die Ereignisanzeige zu sehen, führen Sie **eventvwr.exe** aus oder den Befehl **Systemsteuerung -> Verwaltung -> Ereignisanzeige**.) Sie können die Ereignisse filtern, die geloggt werden.

Sie können die Einstellungen in den Standardoptionen fьr Backup und Recovery exklusiv für die Ereignisse überschreiben, die während eines Backups oder einer Wiederherstellung auftreten. In diesem Fall werden die hier vorgenommenen Einstellungen auch wirksam für andere Tasks, z.B. für die Validierung von Archiven oder die Bereinigung.

Sie können die als Standard gesetzten Optionen auch überschreiben, wenn Sie einen Backup-Plan oder einen Recovery-Task einrichten. Diese so vorgenommenen Einstellungen werden plan-spezifisch oder task-spezifisch verwendet.

Voreinstellung ist: **Ausgeschaltet**.

Wählen Sie das Kontrollkästchen **Ereignisse protokollieren**, um diese Option einzuschalten.

Verwenden Sie das Kontrollkästchen **Ereignisse, die protokolliert werden**, um die Ereignisse zu filtern, die in der Ereignisanzeige von Windows aufgeführt werden:

- **Alle Ereignisse** – loggt alle Ereignisse (Informationen, Warnungen und Fehler)
- **Fehler und Warnungen**
- **Nur Fehler**.

Deaktivieren Sie das Kontrollkästchen **Ereignisse protokollieren**, um diese Option auszuschalten.

14.6.6 Log-Bereinigungsregeln

Diese Option spezifiziert, wie das Log des Acronis Backup & Recovery 11.5 Agenten bereinigt wird.

Diese Option definiert die maximale Größe der Log-Datei des Agenten. Die Dateipfade sind wie folgt:

- In Windows XP und Server 2003: **%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\MMS\events.db3**.
- In Windows Vista und späteren Versionen von Windows: **%PROGRAMDATA%\Acronis\BackupAndRecovery\MMS\events.db3**.
- In Linux: **/var/lib/Acronis/BackupAndRecovery/MMS/events.db3**.

Voreinstellung ist: **Maximale Log-Größe: 50 MB**. **Bei Bereinigung 95% der maximalen Log-Größe bewahren**.

Wenn diese Option aktiviert ist, vergleicht das Programm nach jeweils 100 Log-Einträgen die tatsächliche Log-Größe mit der maximalen Größe. Sobald die maximale Log-Größe überschritten ist, löscht das Programm die ältesten Log-Einträge. Sie können bestimmen, wie viele Log-Einträge beibehalten werden sollen. Mit der Standardeinstellung 95% wird ein Großteil des Logs beibehalten. Mit der Minimaleinstellung 1% wird das Log fast vollständig geleert.

Diesen Parameter können Sie auch im Acronis Administrative Template (S. 448) setzen.

14.6.7 Verwaltung der Maschine

Diese Option legt fest, ob die Maschine zentral durch Acronis Backup & Recovery 11.5 Management Server verwaltet werden muss.

Um diese Option nutzen zu können, müssen Sie als Mitglied der Gruppe der **Administratoren** auf der Maschine angemeldet sein.

Sie können die Maschine auf dem Management Server registrieren, wenn Sie den Acronis Backup & Recovery 11.5 Agent installieren. Wenn die Maschine nicht registriert ist, wählen Sie **Zentrale Verwaltung**, das wird die Registrierung (S. 494) einleiten. Alternativ können Sie die Maschine auch serverseitig im Management Server hinzufügen. Jede der drei beschriebenen Registrierungsmethoden erfordert administrative Berechtigungen.

Die Auswahl von **Autonome Verwaltung** auf einer registrierten Maschine wird die Kommunikation der Maschine mit dem Server stoppen. Die Maschine erscheint als **Zurückgezogen** auf dem Management Server. Der Management Server Administrator kann die Maschine vom Server löschen oder die Maschine erneut registrieren.

Voreinstellung ist: **Autonome Verwaltung**.

So richten Sie die zentrale Verwaltung auf der Maschine ein:

1. Wählen Sie **Zentrale Verwaltung**.

2. Spezifizieren Sie die Angaben für **Management Server IP/Name**.
3. Spezifizieren Sie auf Anforderung den Benutzernamen und das Kennwort des Administrators des Management Servers.
4. Unter **Registrierungsadresse der Maschine** wählen Sie aus, wie die Maschine auf dem Management Server registriert wird: anhand des Namens (empfohlen) oder anhand der IP-Adresse.
5. Klicken Sie auf **OK** und die Maschine wird auf dem Management Server registriert.

Um die zentrale Verwaltung auszuschalten, wählen Sie **Autonome Verwaltung**.

14.6.8 Online Backup-Proxy

Diese Option ist nur wirksam, wenn Backup- und Recovery-Aktionen mit dem Acronis Online Backup Storage über das Internet durchgeführt werden.

Diese Option bestimmt, ob sich der Acronis Agent mit dem Internet über einen Proxy-Server verbinden soll.

Beachten Sie: *Acronis Backup & Recovery 11.5 unterstützt nur HTTP- und HTTPS-Proxy-Server.*

So ändern Sie die Proxy-Server-Einstellungen

1. Aktivieren Sie das Kontrollkästchen **Einen Proxy-Server verwenden**.
2. Geben Sie unter **Adresse** den Netzwerknamen oder die IP-Adresse des Proxy-Servers an – beispielsweise: **proxy.beispielname.com** oder **192.168.0.1**
3. Spezifizieren Sie unter **Port** die Port-Nummer des Proxy-Servers – beispielsweise: **80**
4. Sollte der Proxy-Server eine Authentifizierung benötigen, dann geben Sie die entsprechenden Anmeldedaten unter **Benutzername** und **Kennwort** an.
5. Klicken Sie auf die Schaltfläche **Verbindung testen**, wenn Sie die Proxy-Server-Einstellungen überprüfen wollen.

Wenn Sie die Proxy-Server-Einstellungen nicht kennen, bitten Sie Ihren Netzwerk-Administrator oder Internetzugangsprovider um Unterstützung.

Alternativ können Sie auch versuchen, diese Einstellungen aus der Konfiguration Ihres Webbrowsers zu entnehmen. Die nachfolgenden Befehle zeigen, wo Sie diese in drei populären Webbrowsern finden können.

- **Microsoft Internet Explorer.** Klicken Sie im Menü **Extras** auf den Befehl **Internetoptionen**. Klicken Sie in der Registerlasche **Verbindungen** auf den Befehl **LAN-Einstellungen**.
- **Mozilla Firefox.** Klicken Sie im Menü **Extras** auf den Befehl **Einstellungen** und dann auf **Erweitert**. Klicken Sie in der Registerlasche **Netzwerk**, im Bereich **Verbindung**, auf den Befehl **Einstellungen**.
- **Google Chrome.** Klicken Sie unter **Optionen** auf **Details**. Und im Bereich **Netzwerk** dann auf **Proxy-Einstellungen ändern**.

15 Zentrale Verwaltung

In diesem Abschnitt werden die Aktionen behandelt, die unter Verwendung der Komponenten für die zentrale Verwaltung ausgeführt werden können. Der Inhalt dieses Abschnitts gilt nur für die erweiterten Editionen (Advanced Editions) von Acronis Backup & Recovery 11.5.

15.1 Zentrale Verwaltung verstehen

Dieser Abschnitt enthält einen Überblick über die zentrale Datensicherung mit Acronis Backup & Recovery 11.5. Bevor Sie diesen Abschnitt lesen, sollten Sie wissen, wie Daten auf einer einzelnen Maschine geschьtzt werden.

15.1.1 Grundlegende Konzepte

Zentrale Backup-Pläne erstellen und ihre Ausführung verfolgen

Zum Schutz der Daten einer einzelnen Maschine installieren Sie auf dieser einen Agenten (S. 485) oder multiple Agenten für verschiedene, zu schützende Daten-Typen. Sie verbinden die Konsole mit der Maschine und erstellen einen Backup-Plan (S. 486) oder multiple Backup-Pläne.

Was, wenn Sie mehrere hundert Maschinen zu verwalten haben? Die Erstellung eines Backup-Plans auf jeder Maschine benötigt Zeit, auch wenn die Pläne ähnlich sind – etwa, wenn Sie das System-Laufwerk und die Benutzerdokumente sichern müssen. Genauso zeitaufwendig ist die separate Verfolgung der Plan-Ausführung auf jeder Maschine.

Um die Verwaltungsaktionen auf multiple Maschinen zu übertragen, installieren Sie den Acronis Backup & Recovery 11.5 Management Server (S. 493) und registrieren (S. 494) dann die Maschinen auf diesem Server. Danach können Sie Maschinen-Gruppen erstellen und so multiple Maschinen als Ganzes verwalten. Sie können sie alle zusammen schützen bzw. sichern oder eine bestimmte Auswahl, indem Sie einen zentralen Backup-Plan (S. 396) einrichten.

Sobald Sie die Einrichtung eines zentralen Backup-Plans auf dem Management Server abgeschlossen haben, stellt der Server diesen auf allen im Plan enthaltenen Maschinen bereit. Die Agenten auf den Maschinen starten dann mit der Ausführung des Plans. Sie können den Status des Plans von einer einzelnen Anzeige aus überwachen und bei Bedarf zu jeder Maschine oder jeder Aktivität navigieren, um deren Status und Log-Einträge einzusehen. Der Management Server ermöglicht außerdem, lokal hervorgebrachte Aktivitäten des Agenten zu überwachen und zu verwalten.

Da Sie die Konsole eher mit dem Management Server als mit jeder Maschine verbinden und Sie alle Verwaltungsaktionen durch die zentrale Verwaltungseinheit ausführen, wird diese Art von Verwaltung zentrale Verwaltung (S. 497) genannt.

Eine zentrale Verwaltung schließt nicht die direkte Verwaltung (S. 489) jeder einzelnen Maschine aus. Sie können die Konsole mit jeder Maschine verbinden und jede direkte Verwaltungsaktion durchführen. Zentrale Backup-Pläne können jedoch nur durch den Management Server verwaltet werden, da ein gut durchdachter Plan automatisch funktioniert und nur selten einen menschlichen Eingriff benötigt.

Mit Hilfe des Management Servers können Sie einen oder mehrere zentrale Archiv-Speicher erstellen (zentrale Depots (S. 498)), die von den registrierten Maschinen gemeinsam benutzt werden. Ein zentrales Depot kann von jedem Backup-Plan verwendet werden, egal ob es sich um einen zentralen

Backup-Plan handelt oder einen, der per direkter Verwaltung auf den registrierten Maschinen erstellt wurde.

Einen verwalteten Archiv-Speicher organisieren

Wie groß sollte die Kapazität des zentralen Depots sein? Was, wenn die Übertragung beträchtlicher Backups zum Depot einen Stau im Netzwerk verursacht? Beeinträchtigt das Backup eines in Betrieb befindlichen Produktionsservers seine Performance? Um sicherzustellen, dass das zentrale Backup keine Geschäftsprozesse der Firma ausbremst und um die zum Schutz der Daten benötigten Ressourcen zu minimieren, installieren Sie einen Acronis Backup & Recovery 11.5 Storage Node (S. 495) und konfigurieren ihn zur Verwaltung eines oder multipler zentraler Depots. Solche Depots werden verwaltete Depots (S. 496) genannt.

Der Storage Node hilft dem Agenten, Backups vor Übertragung zu verwalteten Depots zu deduplizieren (S. 488) und dedupliziert selbst bereits in den Depots liegende Backups. Deduplizierung führt zu verringertem Backup-Datentransfer und spart Speicherplatz. Der Storage Node unternimmt außerdem mit Archiven eigene Aktionen (wie Validierung oder Bereinigung), welche ansonsten durch den Agenten ausgeführt werden und befreit so die verwalteten Maschinen von unnötiger Rechenlast. Und nicht zuletzt ermöglicht der Acronis Backup & Recovery 11.5 Storage Node die Verwendung einer Bandbibliothek als verwaltetes Depot für die Speicherung von Backup-Archiven.

Sie können mehr als einen Storage Node, von denen jeder etliche Depots verwaltet, aufsetzen und zentral vom Acronis Backup & Recovery 11.5 Management Server aus steuern.

Zu detaillierten Informationen über Storage Nodes siehe den Abschnitt 'Storage Nodes (S. 247)'.

15.1.2 Rechte für zentrale Verwaltung

Dieser Abschnitt beschreibt die benötigten Benutzerrechte, um eine Maschine lokal oder remote zu verwalten, eine auf dem Acronis Backup & Recovery 11.5 Management Server registrierte Maschine zu verwalten oder um auf einen Acronis Backup & Recovery 11.5 Storage Node zuzugreifen bzw. diesen zu verwalten.

15.1.2.1 Verbindungsarten zu einer verwalteten Maschine

Es gibt zwei Arten von Verbindungen zu einer verwalteten Maschine: lokale Verbindungen und Remote-Verbindungen.

Lokale Verbindung

Eine lokale Verbindung wird auf einer Maschine zwischen der Acronis Backup & Recovery 11.5 Management Console und dem Acronis Backup & Recovery 11.5 Agent auf derselben Maschine aufgestellt.

So stellen Sie eine lokale Verbindung her

- Klicken Sie in der Symbolleiste auf **Verbinden**, anschließend auf **Neue Verbindung** und danach auf **Diese Maschine verwalten**.

Remote-Verbindung

Eine Remote-Verbindung wird zwischen der Acronis Backup & Recovery 11.5 Management Console auf einer Maschine und dem Acronis Backup & Recovery 11.5 Agenten auf einer anderen Maschine etabliert.

Sie müssen möglicherweise zum Aufbau der Remote-Verbindung Anmeldedaten zur Verfügung stellen.

So stellen Sie eine Remote-Verbindung her

1. Klicken Sie in der Symbolleiste auf **Verbinden**, anschließend auf **Neue Verbindung** und danach auf **Eine Remote-Maschine verwalten**.
2. Geben Sie im Feld **Maschine** den Namen oder die IP-Adresse der Remote-Maschine an, zu der Sie sich verbinden wollen oder klicken Sie auf **Durchsuchen**, um die gewünschte Maschine aus einer Liste auszuwählen.
3. Zur Angabe von für die Verbindung benötigten Anmeldedaten klicken Sie auf **Optionen** und geben dann in die Felder **Benutzername** und **Kennwort** die entsprechenden Werte ein. In Windows werden die aktuellen Anmeldedaten verwendet (unter denen die Konsole läuft), falls Sie das Feld **Benutzername** leer lassen.
4. Um das Passwort des angegebenen Benutzernamens zu speichern, aktivieren Sie das Kontrollkästchen **Kennwort speichern**, worauf dieses an einem sicheren Ort auf der Maschine, die die Konsole ausführt, gesichert wird.

15.1.2.2 Rechte für lokale Verbindungen

Windows

Eine lokale Verbindung auf einer unter Windows laufenden Maschine kann von jedem Benutzer etabliert werden, der auf dieser Maschine das Benutzerrecht „lokal anmelden“ hat.

Linux

Für den Aufbau einer lokalen Verbindung auf einer unter Linux laufenden Maschine (und für die Verwaltung dieser Maschine) werden Root-Rechte benötigt.

So stellen Sie eine lokale Verbindung als root her

1. Führen Sie den folgenden Befehl aus, wenn Sie als root angemeldet sind.

   ```
   /usr/sbin/acronis_console
   ```

   Ansonsten führen Sie den folgenden Befehl aus:

   ```
   su -c /usr/sbin/acronis_console
   ```

2. Klicken Sie auf **Diese Maschine verwalten**.

So erlauben Sie einem Benutzer ohne root-Rechte, die Konsole zu starten

- Fügen Sie als root den Namen des Nicht-Root-Benutzers, dem Sie das Ausführen der Konsole erlauben wollen, zur Datei **/etc/sudoers** hinzu – z.B. durch Verwendung des Befehls **visudo**.

***Vorsicht:** Als Folge dieser Prozedur wird dem Nicht-Root-Benutzer nicht nur die Konsolen-Ausführung erlaubt, sondern er kann möglicherweise auch andere Aktionen als „root“ durchführen.*

So stellen Sie als Nicht-Root-Benutzer eine lokale Verbindung her

1. Stellen Sie sicher, dass root Ihnen, wie in der zurückliegenden Prozedur beschrieben, die Berechtigung zum Start der Konsole gegeben hat.
2. Führen Sie den folgenden Befehl aus:

   ```
   sudo /usr/sbin/acronis_console
   ```

3. Klicken Sie auf **Diese Maschine verwalten**.

15.1.2.3 Berechtigungen für Remote-Verbindungen in Windows

Um zu einer unter Windows laufenden Maschine eine Remote-Verbindung aufzubauen, muss der Benutzer auf dieser Maschine Mitglied der Sicherheitsgruppe Acronis Remote Users sein.

Nach Aufbau der Remote-Verbindung hat der Benutzer, wie unter 'Benutzerrechte auf einer verwalteten Maschine (S. 37)' beschrieben, Verwaltungsrechte auf der Remote-Maschine.

Hinweis: *Auf einer Remote-Maschine, die unter Windows Vista (und später) mit eingeschalteter Benutzerkontensteuerung (UAC) läuft und die nicht Teil einer Domain ist, kann nur der standardmäßige Administrator-Benutzer Daten per Backup sichern und Festplattenverwaltungsaktionen ausführen. Sie können diese Beschränkung überwinden, indem Sie die Maschine in eine Domain aufnehmen oder auf der Maschine die Benutzerkontensteuerung (UAC) ausschalten (S. 388) (standardmäßig ist UAC eingeschaltet).*

Zu Informationen über Acronis-Sicherheitsgruppen und ihre Standardmitglieder siehe 'Acronis Sicherheitsgruppen (S. 390)'.

15.1.2.4 Anforderungen an die Benutzerkontensteuerung (UAC)

Zentrale Verwaltungsaktionen (einschließlich Remote-Installationen) erfordern bei Maschinen, die unter Windows Vista (oder höher) laufen und kein Mitglied einer Active Directory-Domain sind, dass die Benutzerkontensteuerung (UAC) deaktiviert ist.

So deaktivieren Sie UAC

Führen Sie in Abhängigkeit vom vorliegenden Betriebssystem einen der nachfolgenden Schritte aus:

- **Bei einem Windows-Betriebssystem vor Windows 8:**

  Gehen Sie zur **Systemsteuerung –> Anzeige: Kleine Symbole –> Benutzerkonten –> Einstellungen der Benutzerkontensteuerung ändern** und ziehen Sie den Schieber auf **Nie benachrichtigen**. Starten Sie die Maschine dann neu.
- **Bei jedem Windows-Betriebssystem**, einschließlich Windows 8/8.1 und Windows Server 2012/2012 R2:
  1. Öffnen Sie den Registrierungseditor.
  2. Suchen Sie folgenden Registry-Schlüssel: **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**
  3. Ändern Sie für den Wert **EnableLUA** die Einstellung auf **0**.
  4. Starten Sie die Maschine neu.

15.1.2.5 Berechtigungen für Remote-Verbindungen in Linux

Remote-Verbindungen zu unter Linux laufenden Maschinen (einschließlich solcher, die von root ausgeführt werden) werden gemäß Authentifizierungsrichtlinien aufgebaut, welche mit Hilfe der „Pluggable Authentication Modules“ für Linux (als Linux-PAM bekannt) eingerichtet werden.

Damit die Authentifizierungsrichtlinien funktionieren, empfehlen wir, die für Ihre Linux-Distribution jeweils aktuellste Linux-PAM-Version zu installieren. Der letzte stabile Source Code von Linux-PAM ist auf der Linux-PAM Source Code Webseite verfügbar.

Remote-Verbindungen als root

Remote-Verbindungen durch den Benutzer 'root' werden gemäß der Authentifizierungsrichtlinie des Acronis Agenten aufgebaut, welche automatisch während der Installation des Acronis Backup & Recovery 11.5 Agenten für Linux eingerichtet wird, indem die Datei '/etc/pam.d/acronisagent' mit folgendem Inhalt erstellt wird:

```
#%PAM-1.0
auth     required     pam_unix.so
auth     required     pam_succeed_if.so uid eq 0
account  required     pam_unix.so
```

Remote-Verbindungen ohne root-Rechte

Weil Systemzugriffe mit root-Rechten die Ausnahme bleiben sollten, kann 'root' eine Authentifizierungsrichtlinie erstellen, damit auch mit „Nicht-root-Anmeldedaten“ eine Remote-Verwaltung möglich ist.

Nachfolgend zwei Beispiele für solche Richtlinien.

Hinweis: *Als Folge sind die spezifizierten 'Nicht-Root'-Benutzer in der Lage, jede Aktion auf der Maschine mit Root-Berechtigungen auszuführen. Es ist gute Praxis sicherzustellen, dass Benutzerkonten nur schwer zu kompromittieren sind – z.B. durch die Anforderung starker Kennwörter*

Beispiel 1

Diese Authentifizierungsrichtlinie verwendet das Modul 'pam_succeed_if' und funktioniert mit Linux-Distributionen mit Kernel 2.6 oder später. Für eine Authentifizierungsrichtlinie, die mit Kernel 2.4 arbeitet, siehe das nächste Beispiel.

Führen Sie folgende Schritte als Benutzer 'root' aus:

1. Erstellen Sie das Gruppen-Konto **Acronis_Trusted**, indem Sie folgenden Befehl ausführen:
   `groupadd Acronis_Trusted`
2. Fügen Sie die Namen der Nicht-Root-Benutzer, denen Sie die Remote-Verbindung zur Maschine erlauben wollen, zur Gruppe **Acronis_Trusted** hinzu. Um den existierenden Benutzer user_a zur Gruppe hinzuzufügen, verwenden Sie z.B. folgenden Befehl:
   `usermod -G Acronis_Trusted user_a`
3. Bearbeiten Sie die Datei '**/etc/pam.d/acronisagent-trusted**' folgendermaßen:

```
#%PAM-1.0
auth      required   pam_unix.so
auth      required   pam_succeed_if.so user ingroup Acronis_Trusted
account   required   pam_unix.so
```

Beispiel 2

Die obere Authentifizierungsrichtlinie funktioniert evtl. nicht unter Linux-Distributionen mit Kernel 2.4 (inkl. Red Hat Linux), weil das Modul 'pam_succeed_if.so' dort nicht unterstützt wird.

In diesem Fall können Sie die folgende Authentifizierungsrichtlinie nutzen:

1. Erstellen Sie als root die Datei **/etc/pam.d/Acronis_trusted_users**
2. Fügen Sie die Namen der Nicht-Root-Benutzer, denen Sie die Verwaltung der Maschine erlauben wollen, der Datei hinzu – ein Benutzername pro Zeile. Um z.B. die Benutzer user_a, user_b und user_c hinzuzufügen, erweitern Sie die Datei um die folgenden drei Zeilen:

```
user_a
user_b
user_c
```

   Sollte es nötig sein, fügen Sie auch root der Datei hinzu.
3. Bearbeiten Sie die Datei '**/etc/pam.d/acronisagent-trusted**' folgendermaßen:

```
#%PAM-1.0
auth     required     pam_unix.so
auth     required     pam_listfile.so item=user sense=allow
file=/etc/pam.d/Acronis_trusted_users onerr=fail
account  required     pam_unix.so
```

15.1.2.6 Acronis Sicherheitsgruppen

Auf einer mit Windows laufenden Maschine bestimmen Acronis Sicherheitsgruppen, wer die Maschine aus der Ferne verwalten und als Acronis Backup & Recovery 11.5 Management Server-Administrator agieren kann.

Diese Gruppen werden erstellt, wenn die Acronis Backup & Recovery 11.5 Agenten oder der Acronis Backup & Recovery 11.5 Management Server installiert werden. Sie können dann während der Installation spezifizieren, welche Benutzer in jede Gruppe aufgenommen werden.

Acronis Backup & Recovery 11.5 Agenten

Bei Installation des Acronis Backup & Recovery 11.5 Agent für Windows auf einer Maschine wird auch die Gruppe **Acronis Remote Users** erstellt (oder aktualisiert).

Ein Benutzer, der Mitglied dieser Gruppe ist, kann die Maschine durch Verwendung der Acronis Backup & Recovery 11.5 Management Console aus der Ferne verwalten, gemäß den unter Benutzerrechte auf einer verwalteten Maschine (S. 37) beschriebenen Verwaltungsrechten.

Standardmäßig enthält diese Gruppe alle Mitglieder der Gruppe Administratoren.

Acronis Backup & Recovery 11.5 Management Server

Wird der Acronis Backup & Recovery 11.5 Management Server auf einer Maschine installiert, so werden dabei zwei Gruppen erstellt (oder aktualisiert):

Acronis Centralized Admins

Ein Benutzer, der Mitglied dieser Gruppe ist, ist ein Management Server Administrator. Management Server Administratoren können sich unter Verwendung der Acronis Backup & Recovery 11.5 Management Console zum Management Server verbinden; sie haben dieselben Verwaltungsrechte auf der registrierten Maschine wie Benutzer mit Administratorrechten auf dieser Maschine – ungeachtet der Inhalte der dortigen Acronis Sicherheitsgruppen.

Damit ein Management Server-Administrator sich auch *remote* mit dem Management Server verbinden kann, muss er außerdem Mitglied der Gruppe Acronis Remote-Benutzer sein.

Kein Benutzer – auch kein Mitglied der Gruppe Administratoren – kann ein Administrator des Management Servers sein, ohne Mitglied der Gruppe Acronis Centralized Admins zu sein.

Standardmäßig enthält diese Gruppe alle Mitglieder der Gruppe Administratoren.

Acronis Remote Users

Ein Benutzer, der Mitglied dieser Gruppe ist, kann sich unter Verwendung der Acronis Backup & Recovery 11.5 Management Console remote zum Management Server verbinden – sofern dieser Benutzer auch Mitglied der Gruppe Acronis Centralized Admins ist.

Standardmäßig enthält diese Gruppe alle Mitglieder der Gruppe Administratoren.

Auf einem Domain-Controller

Ist eine Maschine ein Domain-Controller in einer Active Directory-Domain, so sind die Namen und Standardinhalte der Acronis Sicherheitsgruppen unterschiedlich:

- Anstatt **Acronis Remote Users** und **Acronis Centralized Admins** lauten die Bezeichnungen der Gruppen *DCNAME* **$ Acronis Remote Users** bzw. *DCNAME* **$ Acronis Centralized Admins**; wobei *DCNAME* für den NetBIOS-Namen des Domain-Controllers steht. Jedes Dollar-Zeichen ist auf beiden Seiten von einem Leerzeichen umgeben.
- Statt explizit die Namen aller Mitglieder der Gruppe Administratoren aufzunehmen, wird die Administratoren-Gruppe selbst aufgenommen.

Tipp: *Um ordnungsgemäße Gruppen-Namen zu gewährleisten, sollten Sie eine Acronis-Komponente auf dem Domain-Controller installieren, nachdem Sie diesen aufgesetzt haben. Wurden die Komponenten installiert, bevor Sie den Domain-Controller aufgesetzt haben, so erstellen Sie die Gruppen* DCNAME ***$ Acronis Remote Users*** *und* DCNAME ***$ Acronis Centralized Admins*** *manuell und nehmen dann die Mitglieder von Acronis Remote Users sowie Acronis Centralized Admins in die neu erstellten Gruppen auf.*

15.1.2.7 Rechte des Management Server-Administrators

Normalerweise arbeitet der Acronis Backup & Recovery 11.5 Management Server-Administrator auf einer registrierten Maschine – im Sinne des Acronis Managed Machine Service (auch als Acronis-Dienst) dieser Maschine und mit denselben Rechten, die dieser Dienst hat.

Bei Erstellung eines zentralen Backup-Plans hat der Management Server-Administrator aber auch alternativ die Möglichkeit, explizit ein bestimmtes Benutzerkonto anzugeben, unter dem der zentrale Backup-Plan auf den registrierten Maschinen ausgeführt wird. In diesem Fall muss das Benutzerkonto jedoch auf allen Maschinen vorhanden sein, auf die der zentrale Backup-Plan bereitgestellt wird. Dies ist nicht immer effizient.

Ein Anwender muss, um Management Server-Administrator zu sein, auch Mitglied der Gruppe Acronis Centralized Admins sein – und zwar auf der Maschine, auf der auch der Management Server installiert ist.

15.1.3 Kommunikation zwischen den Komponenten von Acronis Backup & Recovery 11.5

Dieser Abschnitt beschreibt, wie die verschiedenen Komponenten von Acronis Backup & Recovery 11.5 miteinander unter Verwendung sicherer Authentifizierung und Verschlüsselung kommunizieren.

Dieser Abschnitt bietet Ihnen außerdem Informationen über die Konfiguration von Kommunikationseinstellungen, die Wahl eines Netzwerk-Ports zur Kommunikation und die Verwaltung von Sicherheitszertifikaten.

15.1.3.1 Sichere Kommunikation

Acronis Backup & Recovery 11.5 verfügt über die Fähigkeit, die Datenübertragung zwischen seinen Komponenten innerhalb eines Lokalen Netzwerkes (LAN) und durch ein Perimeternetz (auch bekannt als demilitarisierte Zone, DMZ) abzusichern.

Es existieren zwei Mechanismen, um die sichere Kommunikation zwischen den Acronis Backup & Recovery 11.5-Komponenten zu gewährleisten:

- **Sichere Authentifizierung** ermöglicht die sichere Übertragung von zur Etablierung einer Verbindung benötigten Zertifikaten, nämlich durch Verwendung des Secure Sockets Layer-Protokolls (SSL).
- **Verschlüsselte Kommunikation** ermöglicht eine sichere Informationsübertragung zwischen zwei beliebigen Komponenten, z.B. zwischen dem Acronis Backup & Recovery 11.5 Agenten und dem

Acronis Backup & Recovery 11.5 Storage Node, indem die übertragenen Daten verschlüsselt werden.

Zu Anleitungen über das Aufsetzen sicherer Authentifizierung und Daten-Verschlüsselung siehe Kommunikationsoptionen konfigurieren (S. 392).

Zu Anleitungen über die Verwaltung von zur sicheren Authentifizierung eingesetzten SSL-Zertifikaten siehe SSL-Zertifikate (S. 394).

***Beachten Sie:** Die Komponenten früherer Acronis-Produkte, einschließlich solcher aus der Acronis True Image Echo-Familie, können sich nicht mit den Acronis Backup & Recovery 11.5-Komponenten verbinden, ungeachtet der Einstellungen für sichere Authentifizierung und Daten-Verschlüsselung.*

15.1.3.2 Client- und Server-Anwendungen

Es gibt zwei relevante Gruppen beim sicheren Kommunikationsprozess:

- **Client-Anwendung** oder einfach nur Client, womit eine Applikation gemeint ist, die Verbindungen aufzubauen versucht.
- **Server-Anwendung** oder einfach nur Server, womit eine Anwendung gemeint ist, zu der der Client eine Verbindung aufzubauen versucht.

Wenn sich z.B. die Acronis Backup & Recovery 11.5 Management Console zum Acronis Backup & Recovery 11.5 Agenten auf einer Remote-Maschine verbindet, so ist erstere der Client und letztere der Server.

Eine Acronis-Komponente kann als Client- oder Server-Anwendung oder beides agieren, wie der nachfolgenden Tabelle zu entnehmen.

Name der Komponente	Kann Client sein	Kann Server sein
Acronis Backup & Recovery 11.5 Management Console	Ja	Nein
Acronis Backup & Recovery 11.5 Agent	Ja	Ja
Acronis Backup & Recovery 11.5 Management Server	Ja	Ja
Acronis Backup & Recovery 11.5 Storage Node	Ja	Ja
Acronis PXE Server	Nein	Ja
Acronis Backup & Recovery 11.5 Bootable Agent	Ja	Ja

15.1.3.3 Kommunikationseinstellungen konfigurieren

Sie können die Kommunikationseinstellungen (etwa verschlüsselte Datenübertragung) für Acronis Backup & Recovery 11.5-Komponenten (die auf einer oder mehreren Maschinen installiert sind) durch Nutzung von Acronis Administrative Template (administrative Vorlage) konfigurieren. Zu Informationen, wie die administrative Template geladen wird, siehe So laden Sie das Acronis Administrative Template (S. 444).

Wird das administrative Template auf eine Maschine angewendet, so definiert es nur die Kommunikationseinstellungen aller Komponenten dieser Maschine, wird es aber auf eine Domain oder Organisationseinheit angewendet, so definiert es die Kommunikationseinstellungen aller Komponenten von allen Maschinen dieser Domain bzw. Organisationseinheit.

Kommunikationseinstellungen konfigurieren

1. Klicken Sie auf **Start** und dann auf **Ausführen** und geben Sie **gpedit.msc** ein.
2. Erweitern Sie in der **Gruppenrichtlinien**-Konsole den Ast **Computerkonfiguration** und danach den Ast **Administratives Template**, wo Sie auf Acronis klicken.
3. Klicken Sie im rechtsliegenden Acronis-Fensterbereich doppelt auf eine Kommunikationseinstellung, die Sie konfigurieren wollen. Das administrative Template enthält folgende Optionen (S. 445):
   - **Ports für Remote Agent**
   - **Optionen für Client-Verschlüsselung**
   - **Optionen für Server-Verschlüsselung**
4. Starten Sie alle laufenden Acronis-Komponenten neu, bevorzugt durch einen Windows-Neustart, damit die neuen Kommunikationseinstellungen wirksam werden. So gehen Sie vor, wenn kein Neustart möglich ist:
   - Sollte die Acronis Backup & Recovery 11.5 Management Console laufen, so schließen Sie diese und starten sie neu.
   - Sollte eine andere Acronis-Komponente laufen, wie etwa der Acronis Backup & Recovery 11.5 Agent für Windows oder der Acronis Backup & Recovery 11.5 Management Server, so starten Sie deren korrespondierende Dienste mit Hilfe des Snap-ins **Dienste** von Windows neu.

15.1.3.4 Konfiguration des Netzwerk-Ports

Die Komponenten von Acronis Backup & Recovery 11.5 benutzen als Standard den TCP-Port 9876. Der Server lauscht auf diesem Port nach einkommenden Verbindungen. Dieser Port wird außerdem auch als Standard vom Acronis-Client verwendet. Es kann sein, dass Sie während der Installation von Komponenten aufgefordert werden, die Öffnung des Ports zu bestätigen oder den Port manuell zu öffnen, sofern Sie eine andere als die Windows-Firewall verwenden.

Sie können den Port nach der Installation jederzeit wieder auf einen bevorzugten Wert oder zur Erfüllung von Sicherheitszwecken ändern. Diese Aktion benötigt den Neustart des Acronis Remote Agenten (unter Windows) oder des Dienstes acronis_agent (unter Linux).

Nachdem der Port auf der Server-Seite geändert wurde, verbinden Sie sich mit dem Server durch folgende Adress- bzw. URL-Schreibweise: <Server-IP>:<Port> oder <Server-Hostname>:<Port>.

Hinweis: *Falls Sie Network Address Translation (NAT) verwenden, können Sie den Port auch unter Verwendung von Port-Mapping konfigurieren.*

Port-Konfiguration im Betriebssystem

Windows

Um die Port-Nummern ändern zu können, laden und konfigurieren Sie das von Acronis zur Verfügung gestellte aministrative Template, wie es im Abschnitt Kommunikationseinstellungen konfigurieren (S. 392) beschrieben ist.

Linux

Spezifizieren Sie den Port in der Datei /etc/Acronis/Policies/Agent.config. Starten Sie den Daemon 'acronis_agent' neu.

Konfiguration des Ports in einer bootfähigen Umgebung

Sie erhalten während der Erstellung bootfähiger Acronis-Medien die Möglichkeit, die Netzwerkverbindungen vorzukonfigurieren, die vom bootfähigen Acronis Backup & Recovery 11.5 Agent verwendet werden. Es besteht die Wahl zwischen:

- dem Standard-Port (9876)
- dem aktuell verwendeten Port
- dem neuen Port (geben Sie die Port-Nummer ein)

Sofern der Port nicht vorkonfiguriert wurde, verwendet der Agent die Standard-Port-Nummer.

15.1.3.5 SSL-Zertifikate

Die Acronis Backup & Recovery 11.5-Komponten verwenden Secure Sockets Layer (SSL)-Zertifikate für eine sichere Authentifizierung.

Die SSL-Zertifikate für die Komponenten können einer von zwei Typen sein:

- **Selbst-signierte Zertifikate** sind solche Zertifikate, wie sie automatisch während der Installation einer Acronis-Komponente generiert werden.
- **Nicht-selbst-signierte Zertifikate** sind Zertifikate, die durch Dritte, nämlich vertrauenswürdige Zertifizierungsstellen (Certificate Authority, CA) – z.B. VeriSign® oder Thawte™ — oder durch die Zertifizierungsstelle Ihrer Organisation ausgestellt werden.

Zertifikats-Pfad

Alle auf einer Maschine installierten Acronis-Komponenten verwenden, wenn sie als Server-Applikation agieren, ein SSL-Zertifikat, welches als Server-Zertifikat bezeichnet wird.

In Windows werden der Zertifikats-Pfad und der Dateiname des Server-Zertifikates über den Registry-Schlüssel **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Encryption\Server** spezifiziert. Der Standardpfad ist:

- In den 32-Bit-Versionen von Windows: **%CommonProgramFiles%\Acronis\Agent**
- In den 64-Bit-Versionen von Windows: **%CommonProgramFiles(x86)%\AcronisAgent**

Bei selbst-signierten Zertifikaten wird der „Fingerabdruck" des Zertifikats (auch Fingerprint oder Hash genannt) für zukünftige Host-Identifizierung verwendet: Hat sich ein Client schon einmal unter Verwendung eines selbst-signierten Zertifikates mit einem Server verbunden und versucht erneut eine Verbindung aufzubauen, so überprüft der Server, ob der Fingerabdruck des Zertifikates derselbe ist wie beim vorherigen Verbindungsversuch.

Selbst-signierte Zertifikate

Auf unter Windows laufenden Maschinen wird, falls der Zertifikatsspeicher noch kein Server-Zertifikat enthält, ein selbst-signiertes Server-Zertifikat automatisch generiert und eingebunden, sobald irgendeine Acronis-Komponente installiert wird (mit Ausnahme der Acronis Backup & Recovery 11.5 Management Console).

Sollte die Maschine nach Erstellung des selbst-signierten Zertifikates umbenannt werden, so können Sie dieses Zertifikat nicht länger verwenden, sondern müssen ein neues erstellen.

So erstellen Sie ein neues selbst-signiertes Zertifikat

1. Melden Sie sich als Mitglied der Administrator-Gruppe an.
2. Klicken Sie im **Start**-Menü auf **Ausführen** und geben Sie ein: **cmd**

3. Führen Sie folgenden Befehl aus (beachten Sie die Anführungszeichen):
   - Bei Verwendung einer 32-Bit-Version von Windows:
     ```
     "%CommonProgramFiles%\Acronis\Utils\acroniscert" --reinstall
     ```
   - Bei Verwendung einer 64-Bit-Version von Windows:
     ```
     "%CommonProgramFiles(x86)%\Acronis\Utils\acroniscert" --reinstall
     ```
4. Starten Sie Windows oder die laufenden Acronis-Dienste neu.

Nicht-selbst-signierte Zertifikate

Als Alternative zu selbst-signierten Zertifikaten können Sie auch Zertifikate von unabhängigen, vertrauenswürdigen Zertifizierungsstellen (Certificate Authorities, CA) verwenden oder solche, die von der Zertifizierungsstelle Ihrer Firma mit Hilfe von Acronis Certificate Command-line Utility erstellt wurden.

So installieren Sie das Zertifikat einer unabhängigen Zertifizierungsstelle

1. Klicken Sie auf **Start**, dann auf **Ausführen** und geben Sie dort ein: **certmgr.msc**
2. Klicken Sie in der **Zertifikate**-Konsole doppelt auf den Namen des Zertifikates, das Sie installieren wollen.
3. Klicken Sie in der Registerlasche **Details** innerhalb der Liste der angezeigten Felder auf **Fingerabdruck**.
4. Wählen und kopieren Sie den Wert des Feldes (den Zertifikats-Fingerabdruck), eine Zeichenfolge etwa wie **20 99 00 b6 3d 95 57 28 14 0c d1 36 22 d8 c6 87 a4 eb 00 85**.
5. Klicken Sie im Menü **Start** auf **Ausführen** und geben Sie folgendes in die Box **Öffnen** ein (falls Sie eine 64-Bit-Version von Windows verwenden, dann ersetzen Sie **%CommonProgramFiles%** mit **%CommonProgramFiles(x86)%**):
   ```
   "%CommonProgramFiles%\Acronis\Utils\acroniscert.exe" --install "20 99 00
   b6 3d 95 57 28 14 0c d1 36 22 d8 c6 87 a4 eb 00 85"
   ```
   (Beachten Sie die Anführungszeichen, ersetzen Sie den hier gezeigten Beispiels-Fingerabdruck mit dem Ihres tatsächlichen Zertifikates.)

15.2 Backup jetzt

Sie können ein einmaliges Backup von mehreren Maschinen mit ein paar wenigen Schritten konfigurieren, indem Sie die Funktion **Backup jetzt** auf dem Acronis Backup & Recovery 11.5 Management Server verwenden. Der Backup-Prozess wird unmittelbar ausgeführt, sobald Sie alle benötigten Schritte durchgeführt und auf **OK** geklickt haben.

Für längerfristige Backup-Strategien, die Planung und Bedingungen einschließen (etwa zeitbedingtes Löschen oder Verschieben von Backups zu anderen Speicherorten), sollten Sie besser die Erstellung eines Backup-Plans erwägen.

Die Konfiguration eines sofortigen Backups gleicht der Erstellung eines zentralen Backup-Plans (S. 396) mit folgenden Unterschieden:

- Es gibt keine Optionen zur Planung von Backups oder zur Konfiguration von Aufbewahrungsregeln.
- Die Möglichkeit zum Konvertieren eines Laufwerk-Backups zu einer virtuellen Maschine steht nicht als Teil der Backup-Aktion zur Verfügung. Sie können die resultierenden Backups aber anschließend konvertieren.
- Nachdem ein Backup-Task konfiguriert wurde, hat die Software 5 Minuten Zeit, den Task auf den spezifizierten Maschinen bereitzustellen. Sollten während dieses Zeitraums alle Versuche

fehlschlagen, den Task auf einer Maschine bereitzustellen, dann wird diese Maschine nicht per Backup gesichert.

- Wenn Sie denselben Backup-Task erneut ausführen, wird er nur solche Maschinen sichern, die schon bei der ersten Durchführung gesichert wurden.

Anders als eine '**Backup jetzt**'-Aktion, die direkt auf einer verwalteten Maschine (S. 58) ausgeführt wird, verwendet eine auf dem Management Server konfigurierte '**Backup jetzt**'-Aktion niemals die vereinfachte Benennung von Backup-Dateien.

15.3 Erstellung eines zentralen Backup-Plans

Ein zentraler Backup-Plan kann sowohl auf Windows wie auch Linux-Maschinen angewendet werden.

Die zur Erstellung eines zentralen Backup-Plans notwendigen Schritte entsprechen denen bei Erstellung eines Backup-Plans (S. 58), ausgenommen:

- Sie können bei Wahl der Backup-Quelle entweder die Elemente auf den registrierten Maschinen direkt auswählen oder die Auswahlregeln verwenden. Zu weiteren Informationen siehe den Abschnitt 'Daten fьr ein Backup auswдhlen (S. 396)'.
- Bei Angabe des Ziels für die Archive der Maschinen können Sie Folgendes zur Speicherung wählen:
  - Alle Archive der Maschinen an einem einzelnen Ort.
  - Archiv jeder Maschine im angegebenen Ordner auf der Maschine.
  - Das Archiv jeder Maschine in der Acronis Secure Zone der Maschine.

  Zu weiteren Informationen siehe 'Wahl des Speicherorts (S. 404)'.
- **Single-Pass-Laufwerk- und Anwendungs-Backup** (S. 350) steht immer zur Auswahl zur Verfügung. Die Funktion 'Single-Pass-Backup' ist jedoch nur bei solchen Maschinen anwendbar, bei der sie auch möglich ist. Bei durch den Agenten für ESX(i) oder den Agenten für Hyper-V gesicherten virtuellen Maschinen, sowie bei anderen Maschinen, die keine Lizenz für Single-Pass-Backup haben, wird ein reguläres Laufwerk-Backup erstellt.
- Sie können bei Einrichtung einer täglichen, wöchentlichen oder monatlichen Planung die erweiterten Planungseinstellungen verwenden. Zu weiteren Informationen siehe 'Erweiterte Planungseinstellungen (S. 98)'.

15.3.1 Daten für ein Backup auswählen

So wählen Sie Daten für ein Backup aus

1. Bestimmen Sie im Abschnitt **Daten für das Backup** den Typ derjenigen Daten, die Sie sichern wollen. Die Liste der verfügbaren Datentypen hängt von den Agenten ab, die auf den Maschinen laufen:

   Maschinen/Laufwerke/Volumes

   Sie müssen Benutzerrechte als Administrator oder Sicherungs-Operator haben, um diese Daten sichern zu können.

   Wählen Sie diese Option zum Backup:

   - Kompletter physikalischer Maschinen oder einzelner Laufwerke bzw. Volumes von diesen, falls der Acronis Backup & Recovery 11.5 Agent für Windows oder der Acronis Backup & Recovery 11.5 Agent für Linux installiert ist.

     Ein Laufwerk-Backup ermöglicht Ihnen, ein komplettes System auch bei schwerer Datenbeschädigung oder Hardware-Ausfall wiederherzustellen. Sie können außerdem einzelne Dateien und Ordner wiederherstellen. Diese Backup-Prozedur ist schneller als

ein einfaches Kopieren von Dateien und kann Backup-Prozesse beim Sichern großer Datenmengen signifikant beschleunigen.

- Microsoft SQL-Datenbanken mithilfe von Single-Pass-Laufwerk- und Anwendungs-Backup, falls der Acronis Backup & Recovery 11.5 Agent für Microsoft SQL Server (Single-Pass) installiert ist.

  Der Agent für SQL (Single-Pass) ermöglicht Ihnen, applikationskonforme Laufwerk-Backups zu erstellen und Microsoft SQL-Datenbanken von solchen Backups wiederherzustellen. Weitere Informationen finden Sie im Abschnitt 'Microsoft SQL Server schьtzen... (S. 345)'.

- Microsoft Active Directory-Daten mithilfe von Single-Pass-Laufwerk- und Anwendungs-Backup, falls der Acronis Backup & Recovery 11.5 Agent für Microsoft SQL Server (Single-Pass) installiert ist.

  Der Agent für Active Directory (Single-Pass) ermöglicht Ihnen, applikationskonforme Laufwerk-Backups zu erstellen und Microsoft Active Directory-Daten von solchen Backups wiederherzustellen. Weitere Informationen finden Sie im Abschnitt 'Microsoft Active Directory schьtzen... (S. 356)'.

- Kompletter virtueller, auf einem Virtualisierungsserver liegenden Maschinen (oder ihrer Laufwerke bzw. Volumes), falls der Acronis Backup & Recovery 11.5 Agent für ESX(i) oder der Acronis Backup & Recovery 11.5 Agent für Hyper-V installiert ist.

  Das Backup einer kompletten virtuellen Maschine (oder ihrer Laufwerke bzw. Volumes) ergibt standardmäßig ein Laufwerk-Backup (S. 489). Ein solches Backup speichert zudem auch die Konfiguration der virtuellen Maschine. Diese Konfiguration wird Ihnen als Standard vorgeschlagen, wenn Sie den Backup-Inhalt zu einer neuen virtuellen Maschine wiederherstellen wollen. Zu weiteren Informationen über die Sicherung virtueller Maschinen siehe den Abschnitt 'Backups von virtuellen Maschinen'.

Ordner/Dateien

Ist verfügbar, wenn der Acronis Backup & Recovery 11.5 Agent für Windows oder der Acronis Backup & Recovery 11.5 Agent für Linux installiert ist.

Aktivieren Sie diese Option, um spezifische Dateien und Ordner zu sichern.

Ein dateibasiertes Backup ist zur Wiederherstellung eines Betriebssystems nicht ausreichend geeignet. Verwenden Sie ein Datei-Backup, wenn Sie nur bestimmte Daten (beispielsweise ein aktuelles Projekt) sicher bewahren wollen. Das reduziert die Archivgröße und spart so Speicherplatz.

Um Ihr Betriebssystem mit all seinen Einstellungen und Anwendungsprogrammen wiederherstellen zu können, müssen Sie ein Laufwerk-Backup durchführen.

Microsoft Exchange-Informationsspeicher

Ist verfügbar, falls der Acronis Backup & Recovery 11.5 Agent für Microsoft Exchange Server installiert ist.

Wählen Sie diese Option, um den Informationsspeicher, einzelne Speichergruppen oder Datenbanken von Microsoft Exchange-Servern per Backup zu sichern. Im Fall eines Desasters sind Sie in der Lage, verlorene bzw. beschädigte Datenbanken oder Speichergruppen wiederherzustellen. Sie können einzelne Postfächer, Öffentliche Ordner, einzelne E-Mails, Kontakte, Kalenderereignisse und andere Elemente wiederherstellen.

Um Exchange-Daten per Backup sichern zu können, ist ein Domain-Benutzerkonto mit administrativen Berechtigungen auf dem Exchange-Server erforderlich. In einem Cluster muss das Konto über administrative Berechtigungen auf jedem der Cluster-Knoten verfügen.

Zu weiteren Informationen über die Sicherung von Microsoft-Exchange-Daten siehe 'Backups von Microsoft Exchange-Server-Daten'.

Microsoft Exchange-Postfächer

Ist verfügbar, falls der Acronis Backup & Recovery 11.5 Agent für Microsoft Exchange Server installiert ist.

Wählen Sie diese Option, um einzelne Postfächer und Öffentliche Ordner zu sichern, ohne ein Backup der kompletten Microsoft Exchange-Daten durchzuführen. Sie können durch Verwendung von Ausschlussfiltern festlegen, dass bestimmte Elemente bei den Postfach-Backups übersprungen werden.

Um Exchange-Daten per Backup sichern zu können, ist ein Domain-Benutzerkonto mit administrativen Berechtigungen auf dem Exchange-Server erforderlich. In einem Cluster muss das Konto über administrative Berechtigungen auf jedem der Cluster-Knoten verfügen.

Zu weiteren Informationen über die Sicherung von Microsoft-Exchange-Daten siehe 'Backups von Microsoft Exchange-Server-Daten'.

2. Wählen Sie, wie die Elemente ausgewählt werden sollen:
   - **Elemente direkt wählen** (Standardvorgabe) – empfohlen für Fälle, bei denen Sie verschiedene Datenelemente von mehreren Maschinen sichern. Beispielsweise *OrdnerA* von *Maschine1*, *OrdnerB* von *Maschine2*, *OrdnerC* von *Maschine3*, etc.

     Zu sichernde Datenelemente des Microsoft Exchange-Servers werden direkt ausgewählt. Eine Auswahl von Exchange-Datenelementen über Richtlinienregeln wird nicht unterstützt.

     Um alle auf einer Maschine präsenten Elemente des gewählten Datentyps zu sichern, aktivieren Sie das Kontrollkästchen neben der Maschine. Um einzelne Datenelemente zu sichern, müssen Sie die Maschine erweitern und die Kontrollkästchen neben den gewünschten Elementen aktivieren.

     Hinweise für physikalische Maschinen und ihre Laufwerke bzw. Volumes

     - Falls Betriebssystem und Boot-Loader auf unterschiedlichen Volumes liegen, nehmen Sie immer beide mit in das Backup auf. Diese Laufwerke müssen auch zusammen wiederhergestellt werden, da anderenfalls ein hohes Risiko besteht, dass das Betriebssystem nicht mehr startet.
     - Hinweise für Linux-Benutzer: Logische Volumes und MD-Geräte werden unter **Dynamische Volumes** angezeigt. Zu weiteren Informationen über das Backup solcher Volumes und Geräte siehe 'Backup und Recovery von logischen Volumes und MD-Gerдten (Linux) (S. 46)'.
     - Hinweis für Linux-Benutzer: Es wird empfohlen, dass Sie vor dem Backup alle Volumes trennen, die kein Journaling-Dateisystem – wie z.B. ext2 – enthalten. Anderenfalls könnten diese Volumes bei einer Wiederherstellung beschädigte Dateien enthalten; eine Wiederherstellung dieser Volumes bei gleichzeitiger Größenänderung könnte fehlschlagen.

     Hinweise für virtuelle Maschinen und ihre Laufwerke bzw. Volumes

     - Eine Sicherung kompletter virtueller Maschinen ist praktisch, wenn kleine (bezogen auf die virtuelle Laufwerksgröße), aber zahlreiche Legacy-Server vorhanden sind, wie sie aus Systemen zur Server-Auslastung resultieren (Workload-Konsolidierung). Für jede Maschine wird ein separates Archiv erstellt.
     - Eine Sicherung einzelner Laufwerke oder Volumes einer virtuellen Maschine ist praktisch, wenn ein Betriebssystem und Anwendungen (etwa ein Datenbank-Server) auf einem virtuellen Laufwerk liegen, während die Daten (etwa eine Datenbank) auf einem physikalischen, derselben Maschine hinzugefügten Laufwerk mit hoher Kapazität gespeichert sind. Sie können für das virtuelle Laufwerk und den physikalischen Speicher unterschiedliche Backup-Strategien verwenden.

Zu weiteren Informationen über die Sicherung virtueller Maschinen siehe den Abschnitt 'Backups von virtuellen Maschinen'.

- **Richtlinienregeln zur Auswahl verwenden** – empfohlen für Fälle, bei denen Sie die gleichen Datenelemente von mehreren Maschinen sichern. Beispielsweise, um ein Backup des System-Volumes auf jeder gewählten Maschine durchzuführen.

  Siehe folgende Abschnitte für weitere Informationen:

  Auswahlregeln fьr Dateien und Ordner (S. 399)

  Auswahlregeln fьr Volumes (S. 400)

3. Klicken Sie auf **OK**, wenn Sie die Daten für das Backup spezifiziert haben.

15.3.2 Auswahlregeln für Dateien und Ordner

Definieren Sie Auswahlregeln für Dateien, in Übereinstimmung damit, welche Dateien und/oder Ordner von den im zentralen Backup-Plan enthaltenen Maschinen gesichert werden sollen.

So definieren Sie Regeln zur Dateiauswahl

1. Wählen Sie die Regel aus dem Listenfeld (oder geben Sie sie manuell ein) und klicken Sie dann auf **Regel hinzufügen**. Das Programm merkt sich manuell eingegebene Regeln, und wenn Sie das nächste Mal das Fenster öffnen, stehen diese zusammen mit den Standardregeln zur Auswahl in der Liste bereit.
2. Aktivieren Sie im rechten Fensterbereich die Kontrollkästchen neben den Maschinen oder Gruppen, auf die sie die Regeln anwenden wollen.

Windows

Vollständiger Pfad

Wählen Sie die zu sichernden Dateien und Ordner. Wenn Sie explizit einen Pfad zu einer Datei bzw. Ordner spezifiziert haben, dann wird der Plan dieses Element von jeder Maschine sichern, auf der genau dieser Pfad gefunden wird.

Mit einbeziehen	In der Spalte „Dateien und Ordner" geben Sie Folgendes ein oder wählen es aus:
Datei Text.doc im Ordner D:\Arbeit	**D:\Arbeit\Text.doc**
Ordner C:\Windows	**C:\Windows**

Umgebungsvariablen

Manche Umgebungsvariablen verweisen auf Windows-Ordner. Die Verwendung solcher Variablen statt vollständiger Datei- und Verzeichnis-Pfade, stellt die Sicherung der richtigen Windows-Ordner sicher, unabhängig davon, wo Windows auf einer bestimmten Maschine lokalisiert ist.

Mit einbeziehen	In der Spalte „Dateien und Ordner" geben Sie Folgendes ein oder wählen es aus	Kommentare
Ordner „Programme"	**%PROGRAMFILES%**	Verweist auf den Ordner für Programme (z.B. **C:\Programme**)
Windows-Ordner	**%WINDIR%**	Verweist auf den Ordner, wo Windows gespeichert ist (z.B. **C:\Windows**)

Allgemeine Daten für alle Benutzerprofile	**%ALLUSERSPROFILE%**	Verweist auf den Ordner, wo die allgemeinen Daten für alle Benutzerprofile hinterlegt sind, (**C:\Dokumente und Einstellungen\All Users** in Windows XP und **C:\Users bzw. C:\Benutzer** in Windows Vista und Windows 7)

Sie können auch andere Umgebungsvariablen oder eine Kombination von Umgebungsvariablen und Text verwenden. Um z.B. auf den Ordner „Acronis“ im Ordner „Programme“ der Maschine zu verweisen, geben Sie ein: **%PROGRAMFILES%\Acronis**

Templates

Templates sind ähnlich zu Umgebungsvariablen, aber bereits vorangepasst.

Mit einbeziehen	In der Spalte „Dateien und Ordner“ geben Sie Folgendes ein oder wählen es aus:	Kommentare
Alle Dateien auf allen Volumes einer Maschine	**[Alle Dateien]**	Verweist auf alle Dateien auf allen Volumes der Maschine.
Alle auf einer Maschine existierenden Benutzerprofile	**[Alle Benutzerprofile-Ordner]**	Verweist zum Ordner, in dem alle Benutzerprofile gespeichert sind (z.B. **C:\Dokumente und Einstellungen** in Windows XP und **C:\Users bzw. C:\Benutzer** in Windows Vista und Windows 7).

Linux

Mit einbeziehen	In der Spalte „Dateien und Ordner“ geben Sie Folgendes ein oder wählen es aus:
Die Textdatei „Datei.txt“ auf der Partition „/dev/hda3“, gemountet an „/home/usr/docs“	**/dev/hda3/Datei.txt** oder **/home/usr/docs/Datei.txt**
Home-Verzeichnis der allgemeinen Benutzer	**/home**
Das Heim-Verzeichnis des Benutzers „root“.	**/root**
Verzeichnis für alle Benutzer-bezogenen Programme	**/usr**
Verzeichnis für System-Konfigurationsdateien	**/etc**

15.3.3 Auswahlregeln für Volumes

Definieren Sie Volume-Auswahlregeln, gemäß derer die Volumes der Maschinen, welche im zentralen Backup-Plan enthalten sind, gesichert werden sollen.

So definieren Sie Regeln zur Laufwerksauswahl

1. Wählen Sie die Regel aus dem Listenfeld (oder geben Sie sie manuell ein) und klicken Sie dann auf **Regel hinzufügen**. Das Programm merkt sich manuell eingegebene Regeln, und wenn Sie das nächste Mal das Fenster öffnen, stehen diese zusammen mit den Standardregeln zur Auswahl in der Liste bereit.
2. Aktivieren Sie im rechten Fensterbereich die Kontrollkästchen neben den Maschinen oder Gruppen, auf die sie die Regeln anwenden wollen.

Die folgende Tabelle erläutert die vordefinierten, von der Liste auswählbaren Regeln. Namen von Templates unterscheiden Groß-/Kleinschreibung.

Mit einbeziehen	In der Box für die Auswahlregeln:	Kommentare
	Windows- und Linux-Partitionen	
Alle Volumes	Geben Sie ein oder wählen Sie aus: **[Alle Volumes]**	Bezieht sich auf alle Partitionen von Maschinen, die unter Windows laufen – und auf alle gemounteten Partitionen von Maschinen, die unter Linux laufen.
	Windows-Partitionen	
Partition C:	Geben Sie **C:** ein oder wählen Sie die Partition von der Liste	
Systempartition	Geben Sie ein oder wählen Sie aus: **[SYSTEM]**	Das System-Volume enthält die Hardware-spezifischen Dateien, die zum Start von Windows benötigt werden, wie Ntldr, Boot.ini und Ntdetect.com. Es gibt nur ein System-Volume, selbst wenn mehrere Windows-Betriebssysteme auf dem Computer installiert sind. Zu mehr Details siehe „Bemerkungen zu Windows-Maschinen".
Boot-Volume	Geben Sie ein oder wählen Sie aus: **[BOOT]**	Bezieht sich auf die Boot-Partition der registrierten Maschine. Die Boot-Partition enthält den Windows-Ordner und die dazugehörigen Dateien für das Windows-Betriebssystem (üblicherweise im Ordner Windows\System32 liegend). Es kann, muss sich aber nicht um dasselbe Laufwerk wie die Systempartition handeln. Sind mehrere Betriebssysteme auf dem Computer installiert, dann ist dies die Boot-Partition des Betriebssystems, in dem der Agent arbeitet. Zu mehr Details siehe „Bemerkungen zu Windows-Maschinen".
Alle fest eingebauten Laufwerke	Geben Sie ein oder wählen Sie aus: **[Fest eingebaute Volumes]**	Bezieht sich auf alle Volumes außer Wechselmedien. Fest eingebaute Volumes beinhalteten Volumes auf SCSI-, ATAPI-, ATA-, SSA-, SAS- und SATA-Geräten sowie auf RAID-Arrays.
Erstes Laufwerk	Geben Sie ein oder wählen Sie aus: **[Laufwerk 1]**	Bezieht sich auf das erste Laufwerk der registrierten Maschine, einschließlich aller Volumes auf diesem Laufwerk.

Linux-Partitionen		
Erste Partition auf der ersten IDE-Festplatte einer Linux-Maschine	Geben Sie ein oder wählen Sie aus: **/dev/hda1**	hda1 ist der Standard-Gerätename für die erste Partition der ersten IDE-Festplatte. Zu mehr Details siehe „Bemerkungen zu Linux-Maschinen“.
Erste Partition auf der ersten SCSI-Festplatte einer Linux-Maschine	Geben Sie ein oder wählen Sie aus: **/dev/sda1**	sda1 ist der Standard-Gerätename für die erste Partition der ersten SCSI-Festplatte. Zu mehr Details siehe „Bemerkungen zu Linux-Maschinen“.
Erste Partition auf der ersten Software-RAID-Festplatte einer Linux-Maschine	Geben Sie ein oder wählen Sie aus: **/dev/md1**	md1 ist der Standard-Gerätename für die erste Partition des ersten Software-RAID-Laufwerkes. Zu mehr Details siehe „Bemerkungen zu Linux-Maschinen“.

Bemerkungen zu Windows-Maschinen

Bei Windows-Versionen vor Windows 7 und Windows Server 2008 R2 liegen Systemdateien und Boot-Loader auf demselben Volume, es sei denn, während der Systeminstallation wurde explizit ein anderes Volume angegeben. Wenn sich die Windows-Dateien und der Loader auf demselben Volume befinden, ist die je einzelne Auswahl der Option **[SYSTEM]** oder **[BOOT]** ausreichend, um das Betriebssystem vollständig zu sichern. Anderenfalls wählen Sie sowohl **[SYSTEM]** als auch **[BOOT]**.

Beginnend mit Windows 7 und Windows Server 2008 R2 erstellen diese Betriebssystem-Versionen bei Ihrer Installation auf einem neuen Laufwerk ein dediziertes System-Volume mit der Kennzeichnung **System-reserviert**. Wenn Sie **[SYSTEM]** wählen, wird nur dieses dedizierte Volume gesichert. Wählen Sie immer sowohl **[SYSTEM]** als auch **[BOOT]**, wenn Sie Maschinen mit diesen Betriebssystemen sichern.

Weil zentrale Backup-Pläne üblicherweise viele Maschinen mit unterschiedlichen Betriebssystemen enthalten, empfiehlt Acronis, immer sowohl das System- wie auch das Boot-Volume zum Backup auszuwählen. Dies gewährleistet die Integrität jedes Betriebssystems.

Bemerkungen zu Linux-Maschinen

Sie können Windows- und Linux-Volumes (Partitionen) gemeinsam in eine zentrale Backup-Richtlinie aufnehmen.

Es ist beispielsweise möglich, einen zentralen Backup-Plan zu konfigurieren, der Volume **C:** auf Windows-Maschinen und Volume (Partition) **/dev/hda1** auf Linux-Maschinen sichert.

Anders als bei Windows gibt es in Linux keine klare Unterscheidung zwischen einem Volume (Partition) und einem Ordner (Verzeichnis). Linux hat ein Root-Volume (als / gekennzeichnet), an das Elemente verschiedenen Typs – inkl. Festplattenlaufwerke, Verzeichnisse und Systemgeräte – angeschlossen werden (gemountet). Dadurch wird ein Verzeichnisbaum erstellt, der der Datei- und Ordner-Struktur von Windows ähnlich ist.

Lassen Sie z.B. eine Linux-Maschine ein Laufwerk enthalten, das in drei Volumes (bzw. Partitionen) aufgeteilt ist: die erste, zweite und dritte Partition. Diese Partitionen (Volumes) sind im Verzeichnisbaum als /dev/hda1, /dev/hda2 bzw. /dev/hda3 verfügbar. Um z.B. ein Laufwerk-Backup des dritten Volumes (Partition) durchzuführen, können Sie **/dev/hda3** als Regel in der Dialogbox **Daten für das Backup** spezifizieren.

Ein Linux-Volume kann außerdem irgendwo innerhalb des Verzeichnisbaums gemountet werden. So kann beispielsweise '/dev/hda3' als Unterverzeichnis innerhalb dieses 'Baums' gemountet sein. Ein solcher 'Baum' kann beispielsweise '/home/usr/docs' sein. In diesem Fall können Sie entweder

'/dev/hda3' oder '/home/usr/docs' in das Feld 'Volume' eingeben, um ein Laufwerk-Backup des dritten Volumes durchzuführen.

Im Allgemeinen sollten Sie beim Aufsetzen eines zentralen Backup-Plans zur Durchführung von Laufwerk-Backups auf Linux-Maschinen sicherstellen, dass die bei den Auswahlregeln für die Volumes eingegebenen Pfade mit entsprechenden Partitionen (wie '/dev/hda2' oder '/home/usr/docs' aus dem vorherigen Beispiel) und nicht Verzeichnissen korrespondieren.

Standardnamen für Linux-Volumes (Partitionen)

Namen wie **/dev/hda1** reflektieren die übliche Art, die Volumes (Partitionen) von IDE-Laufwerken in Linux zu bezeichnen. Das Präfix **hd** kennzeichnet den Laufwerkstyp (IDE) – wobei **a** bedeutet, dass es das erste IDE-Laufwerk des Systems ist und **1** das erste Volume (Partition) auf dem Laufwerk bezeichnet.

Im Allgemeinen besteht der Standardname für ein Linux-Volume aus drei Komponenten:

- **Laufwerkstyp:** 'hd' für IDE-Laufwerke, 'sd' für SCSI-Laufwerke und 'md' für Software-RAID-Laufwerke (z.B. dynamische Volumes)
- **Laufwerksnummer:** 'a' für das erste Laufwerk, 'b' für das zweite usw.
- **Partitionsnummer auf dem Laufwerk:** 1 für die erste Partition (Volume), 2 für die zweite Partition (Volume), usw.

Um ein Backup ausgewählter Laufwerke unabhängig von ihrem Typ zu garantieren, sollten Sie erwägen, drei Einträge in die Dialogbox **Daten für das Backup** aufzunehmen, einen für jeden möglichen Typ. Um beispielsweise das erste Laufwerk einer jeden Linux-Maschine unter einem zentralen Backup-Plan zu sichern, können Sie folgende Regeln hinzufügen:

/dev/hda1

/dev/sda1

/dev/mda1

Namen für logische Volumes

Um logische Volumes (auch LVM-Volumes genannt) zu sichern, müssen Sie deren vollständige Namen in den Auswahlregeln spezifizieren: Der vollständige Name eines logischen Volumes beinhaltet die Volume-Gruppe, zu der das Volume gehört.

Spezifizieren Sie als Beispiel folgende Auswahlregeln, um zwei logische Volumes namens **lv_root** und **lv_bin** – beide zur Volume-Gruppe **vg_mymachine** gehörend – zu sichern:

```
/dev/vg_mymachine/lv_root
/dev/vg_mymachine/lv_bin
```

Verwenden Sie das Utilitiy **lvdisplay**, um auf einer Maschine eine Liste der logischen Volumes einzusehen. In unserem Beispiel sieht die Ausgabe ungefähr wie folgt aus:

```
--- Logical volume ---
LV Name          /dev/vg_mymachine/lv_root
VG Name          vg_mymachine
…

--- Logical volume ---
LV Name          /dev/vg_mymachine/lv_bin
VG Name          vg_mymachine
…
```


15.3.4 Auswahl der Backup-Speicherortes

Geben Sie an, wo die Archive gespeichert werden sollen und definieren Sie Namen für die neuen Backup-Archive.

1. Das Ziel für die Archive wählen

Wählen Sie, wo die Archive der Maschinen gespeichert werden:

- **Alle Archive der Maschinen an einem einzelnen Ort speichern**
  - Klicken Sie zur Speicherung von Backups auf dem Acronis Online Backup Storage auf **Anmelden**, geben Sie anschließend die Anmeldedaten zum Zugriff auf den Online Storage ein. Erweitern Sie dann die Gruppe **Online Backup Storage** und wählen Sie das Konto.

    Bevor Sie Ihre Backups auf dem Online Storage sichern können, müssen Sie für den Online Backup-Dienst ein Abonnement kaufen (S. 475) und das Abonnement auf der zu sichernden Maschine aktivieren (S. 477). Die Online Backup-Funktion steht unter Linux nicht zur Verfügung.

    Acronis Backup & Recovery Online ist möglicherweise in Ihrer Region nicht verfügbar. Zu weiteren Informationen klicken Sie hier: http://www.acronis.de/my/backup-recovery-online/

  - Um Archive in einem zentralen Depot zu speichern, erweitern Sie die Gruppe **Depots** und klicken auf das entsprechende Depot.
  - Um die Archive auf einer Netzwerkfreigabe zu sichern, erweitern Sie die Gruppe **Netzwerk-Ordner**, wählen dann die benötigte Netzwerk-Maschine und klicken dann auf den freigegebenen Ordner. Werden Anmeldedaten zum Zugriff auf die Netzwerkfreigabe benötigt, so wird das Programm diese erfragen.
  - Um die Archive auf einem **FTP-** oder **SFTP-**Server zu speichern, erweitern Sie die korrespondierende Gruppe und greifen auf den entsprechenden Server zu, wo Sie dann den zum Speichern verwendeten Ordner wählen.

    Entsprechend der FTP-Spezifikation werden Anmeldedaten zum Zugriff auf einen FTP-Server als Klartext über das Netzwerk versendet. Benutzername und Kennwort könnten also jederzeit mit einem Packet-Sniffer abgefangen werden.

- **Archiv jeder Maschine im angegebenen Ordner auf der Maschine mit Agent speichern**

  Geben Sie den vollständigen Pfad zu dem Ordner im Feld **Pfad** an. Sie müssen diesen Ordner im Voraus auf jeder Maschine erstellen, für die der zentrale Plan erstellt wurde.

- **Archiv aller Maschinen in der Acronis Secure Zone der Maschine speichern**

  Sie müssen die Acronis Secure Zone im Voraus auf jeder Maschine erstellen, für die der zentrale Plan erstellt wurde. Zu weiteren Informationen über die Erstellung der Acronis Secure Zone siehe den Abschnitt Acronis Secure Zone erstellen (S. 218).

2. Die Archive benennen

Die Daten jeder Maschine werden zu einem separaten Archiv gesichert.

Die Software generiert einen einheitlichen Namen für die neuen Archive und zeigt diesen im Feld **Name** an. Der Name sieht aus wie *[Maschinenname]_Archiv(N)*, wobei *[Maschinenname]* für die Bezeichnung der Maschine steht (physikalisch oder virtuell) und *N* eine fortlaufende Nummer ist. Sind Sie mit dem automatisch generierten Namen nicht einverstanden, so konstruieren Sie einen anderen.

Bei der Auswahl von Daten zum Backup mehrerer Maschinen können Sie folgende Variablen verwenden:

- [Machine Name] – Platzhalter für den Namen der Maschine. Die Verwendung dieser Variable ist zwingend.
- [Plan name] – Platzhalter für den Namen des zentralen Backup-Plans. Verwenden Sie diese Variable zur zusätzlichen Unterscheidung der Archive anhand des Backup-Plan-Namens.
- [Virtual Host Name] – Platzhalter für den Namen des Hosts der virtuellen Maschine. Verwenden Sie diese Variable in Fällen, in denen zwei oder mehrere virtuelle Maschinen von unterschiedlichen Hosts denselben Namen haben.

Beispiel: Sie erstellen einen zentralen Backup-Plan mit den Namen *SYSTEMBACKUP*, der auf drei Maschinen bereitgestellt wird (beispielsweise *FINABT1*, *FINABT2*, *FINABT3*). Sie spezifizieren im Feld **Name** die Variablen *[Maschinenname]_[Plan-Name]_Archiv(N)*. Dadurch werden im Speicherort die folgenden drei Archive erstellt:

- FINABT1_SYSTEMBACKUP_Archiv(1)
- FINABT2_SYSTEMBACKUP_Archiv(1)
- FINABT3_SYSTEMBACKUP_Archiv(1)

15.3.5 Anmeldedaten des zentralen Backup-Plans

Geben Sie die Anmeldedaten ein, unter denen die zentralen Tasks auf den Maschinen laufen werden.

So spezifizieren Sie Anmeldedaten

1. Wählen Sie eine der nachfolgenden Varianten:
   - **Anmeldedaten des Acronis-Dienstes verwenden**

     Die Tasks werden unter dem Konto des Acronis-Dienstes ausgeführt, egal ob manuell oder per Zeit-/Ereignis-Planung gestartet.
   - **Folgende Anmeldedaten verwenden**

     Die Tasks werden mit den von Ihnen spezifizierten Anmeldedaten ausgeführt, egal ob manuell oder per Zeit-/Ereignis-Planung gestartet.

     Spezifizieren Sie:
     - **Benutzername**. Stellen Sie sicher, dass Sie auch den Domain-Namen spezifizieren (DOMAIN\Benutzername oder Benutzername@domain), wenn Sie den Namen eines Active Directory-Benutzerkontos eingeben.
     - **Kennwort**. Das Kennwort für das Konto.
     - **Kennwort bestätigen**. Geben Sie das Kennwort erneut ein.
2. Klicken Sie auf **OK**.

Um mehr über Anmeldedaten für die Dienste von Acronis zu erfahren, siehe den Abschnitt 'Liste der Acronis Services (Dienste) (S. 38)'.

Siehe den Abschnitt 'Benutzerberechtigungen auf einer verwalteten Maschine (S. 37)', um mehr über Aktionen zu erfahren, die in Abhängigkeit von Benutzerberechtigungen verfügbar sind.

15.3.6 Was, wenn eine Maschine keine Daten hat, die mit den Auswahlregeln übereinstimmen?

Ein zentraler Backup-Plan kann auf eine Maschine bereitgestellt werden, die über keine mit den Auswahlregeln übereinstimmenden Daten verfügt. Beim Deployment des Plans werden keine Fehler oder keine Warnung aufgezeichnet, da angenommen wird, dass die Daten noch zukünftig auftauchen

können. Wie üblich wird ein Backup-Plan erstellt und das Stadium des Plans wechselt zu **Bereitgestellt**.

Falls beim Start des Backup-Tasks keine zu sichernden Daten gefunden werden, schlägt der Task fehl und der Plan-Status wechselt zu **Fehler**. Wenn wenigstens eines der Daten-Elemente gefunden wird, wird der Backup-Task mit einer Warnmeldung erfolgreich abgeschlossen. Der Plan-Status ändert sich entsprechend.

Die Backup-Tasks starten planmäßig (wie durch den Plan spezifiziert) und produzieren solange ein vergleichbares Ergebnis, bis alle Daten-Elemente auf der Maschine auftauchen oder der Plan so bearbeitet wird, dass die nicht existierenden Daten-Elemente ausgeschlossen werden.

Beispiele

Angenommen, die Auswahlregel legt fest, dass der Plan die Laufwerke D: und F: sichern soll. Die Richtlinie wird auf Linux- und Windows-Maschinen gleichermaßen bereitgestellt. Sobald das erste Backup gestartet ist, erhält der Plan auf Linux-Maschinen den Status **Fehler** – wie auch auf Windows-Maschinen, die keine entsprechenden Volumes haben. Der Plan erhält den Status **Warnung** auf solchen Windows-Maschinen, die entweder ein D:- oder F:- Volume haben, es sei denn, ein Fehler-produzierendes Ereignis tritt auf.

Der Plan, der die Volumes [SYSTEM] und '/dev/sda1' sichern muss, wird auf den Windows-Maschinen den Status **Warnung** erhalten (da '/dev/sda' nicht gefunden wird) – genauso wie auf den Linux-Maschinen, die nur das Laufwerk '/dev/sda1' haben. Denn hier wird das Volume [SYSTEM] nicht gefunden. Auf Linux-Maschinen, die kein SCSI-Gerät haben, erhält der Plan den Status **Fehler**.

15.4 Acronis Backup & Recovery 11.5 Management Server administrieren

In diesem Abschnitt werden die Ansichten beschrieben, die über den Naivigationsbaum eines mit der Konsole verbundenen Management Servers verfügbar werden und erklärt, wie Sie mit diesen Ansichten arbeiten.

15.4.1 Dashboard

Verwenden Sie die Ansicht **Dashboard**, um auf einen Blick den Status der Datensicherung auf registrierten Maschinen einschätzen zu können. Das Dashboard zeigt eine Zusammenfassung aller Aktivitäten der Acronis Backup & Recovery 11.5 Agenten an, lässt Sie den freien Speicherplatz der verwalteten Depots überprüfen sowie Probleme schnell erkennen und beheben.

Neueste Alarmmeldungen

Im Bereich **Neueste Alarmmeldungen** werden Sie über Probleme informiert, die in zentralen Depots, auf dem Management Server und auf registrierten Maschinen aufgetreten sind. Sie erhalten die Möglichkeit, die Probleme zu untersuchen oder zu lösen. Standardmäßig werden in diesem Bereich die fünf neuesten Alarmmeldungen angezeigt. Klicken Sie auf den Link **Alle anzeigen**, um zur Ansicht **Alarmmeldungen** zu gelangen und alle Alarmmeldungen sehen zu können. Falls keine Alarm- oder Warnmeldungen erfasst wurden, zeigt das System „Es gibt keine Alarmmeldungen“ an.

Aktivitätsverlauf

Im Säulendiagramm des Abschnitts **Aktivitätsverlauf** können Sie den täglichen Verlauf aller Aktivitäten der Acronis Backup & Recovery 11.5 Agenten untersuchen. Der Verlauf basiert auf den Log-Einträgen, die auf den registrierten Maschinen und auf dem Management Server erfasst wurden.

Das Diagramm zeigt die Anzahl der Log-Einträge eines jeden Typs (**Erfolgreich abgeschlossen**, **Mit Warnungen**, **Fehlgeschlagen**) für einen bestimmten Tag an.

Die Statistik für das ausgewählte Datum wird rechts vom Diagramm angezeigt. Alle Felder in der Statistik sind interaktiv, d.h. wenn Sie also auf ein Feld klicken, wird die Ansicht **Log** geöffnet und in dieser sind die Log-Einträge nach dem betreffenden Feld vorgefiltert.

Im oberen Bereich des Diagramms können Sie die Aktivitäten auswählen, die in Abhängigkeit von der Anwesenheit und dem Schweregrad der Fehler ausgeführt werden sollen. Klicken Sie auf den Link **Alle anzeigen**, damit in der Ansicht **Log** alle Aktivitäten angezeigt werden. Sie werden nach ihrem Startzeitpunkt sortiert. Wenn Sie mit der rechten Maustaste im Säulendiagramm auf einen bestimmten Tag klicken, wird ein Kontextmenü angezeigt und können Sie für den gewählten Tag zur Ansicht **Log** wechseln.

Die Schaltfläche **Aktueller Tag** fokussiert die Auswahl auf den aktuellen Tag.

Maschinen, Backup-Pläne und Recovery-Tasks

In den Abschnitten **Maschinen**, **Backup-Pläne** und **Recovery-Tasks** werden zusammenfassende Statistiken für die registrierten Maschinen, Backup-Pläne und Recovery-Tasks angezeigt. Klicken Sie auf die Elemente dieser Abschnitte, um die relevanten Informationen zu erhalten. Auf diese Weise gelangen Sie zur entsprechenden Ansicht mit den vorgefilterten Maschinen, Backup-Plänen bzw. Recovery-Tasks. Wenn Sie beispielsweise unter **Recovery-Tasks** auf **Benutzereingriff erforderlich** klicken, wird die Ansicht **Backup-Pläne und Tasks** geöffnet, wobei die Recovery-Tasks nach dem Stadium **Benutzereingriff erforderlich** gefiltert sind.

Die in den Abschnitten **Maschinen**, **Backup-Pläne** und **Recovery-Tasks** präsentierten Informationen werden jedes Mal aktualisiert, wenn sich der Management Server mit den Maschinen synchronisiert. Die Informationen in den anderen Abschnitten werden alle 10 Minuten sowie jedes Mal, wenn Sie auf das Dashboard zugreifen, aktualisiert.

Applikationen

Der Abschnitt **Applikationen** zeigt die Anzahl der geschützten und ungeschützten Anwendungen an, die auf den registrierten Maschinen laufen.

Eine Applikation auf einer Maschine wird als 'geschützt' angesehen, falls der entsprechende Agent auf dieser Maschine im Testmodus oder mit einem Lizenzschlüssel installiert ist. Falls ein Agent im Modus 'Nur Online Backups' installiert ist, wird die Applikation nicht als geschützt angesehen.

Folgende Applikationen können geschützt werden:

- Microsoft Active Directory
- Microsoft Exchange Server
- Microsoft SQL Server (mehrere SQL Server-Instanzen werden als eine Applikation gezählt)

Sie können eine Liste von Maschinen mit ungeschützten Applikationen einsehen, wenn Sie auf **Ungeschützte Applikationen** klicken.

Depots

Im Abschnitt **Depots** werden die Informationen zur Speicherplatznutzung der Depots angezeigt. In einigen Fällen ist die Information zum freien Speicherplatz in einem Depot möglicherweise nicht verfügbar, z.B. dann, wenn sich das Depot in einer Bandbibliothek befindet (Banddepot). Wenn das Depot selbst nicht verfügbar (offline) ist, dann wird die Meldung „Depot ist nicht verfügbar“ angezeigt.

Falls es keine Depots gibt, wird die Meldung „Es wurden keine zentralen Depots erstellt“ angezeigt. Wählen Sie zur Erstellung eines neuen Depots den Link **Jetzt erstellen** und wechseln Sie so zur Seite **Depot erstellen**.

15.4.2 Maschinen mit Agenten

Mit Acronis Backup & Recovery 11.5 können Sie Ihre Daten schützen bzw. sichern und Verwaltungsaktionen mit mehreren Maschinen ausführen.

Fьgen Sie eine Maschine (S. 412) dem Management Server durch Angabe ihres Namens oder ihrer IP-Adresse hinzu und importieren Sie Maschinen aus dem Active Directory oder aus einer Textdatei. Sobald eine Maschine auf dem Management Server registriert ist, wird sie für zentrale Backups (S. 396), Gruppierung sowie Überwachung ihrer Aktivitäten verfügbar.

Um einzuschätzen, ob die Daten einer verwalteten Maschine erfolgreich geschützt bzw. gesichert sind, überprüfen Sie ihren Status. Der Status einer Maschine wird definiert durch den schwerwiegendsten Status aller Backup-Plдne (S. 364) (lokal und zentral), der auf der Maschine vorhanden ist. Er kann die Werte 'OK', 'Warnung' oder 'Fehler' annehmen.

Typischer Arbeitsablauf

- Erstellen Sie eine benutzerdefinierte Gruppe und fügen Sie dieser Maschinen hinzu. Zu weiteren Informationen siehe 'Maschinengruppen (S. 408)'.
- Wählen Sie eine Maschine (oder Gruppe) aus, um Aktionen auf diese anwenden zu können. Siehe 'Aktionen mit Maschinen (S. 409)' und 'Aktionen mit Gruppen (S. 417)'.
- Um detaillierte Informationen über eine gewählte Maschine (oder Gruppe) einzusehen und zusätzliche Aktionen ausführen zu können (wie etwa Tasks auszuführen/stoppen oder Backup-Pläne zu importieren/exportieren), verwenden Sie den Informationsbereich im unteren Teil des Fensters. Die Leiste ist standardmäßig eingeklappt. Sie können den Fensterbereich aufklappen, indem Sie auf das Pfeilsymbol klicken.
- Verwenden Sie die Möglichkeit zum Filtern und Sortieren, um die gewünschten Maschinen einfacher durchsuchen und überprüfen zu können. Zu weiteren Informationen siehe 'Tabellenelemente sortieren, filtern und konfigurieren (S. 29)'.

15.4.2.1 Maschinengruppen

Maschinengruppen wurden entworfen, um eine große Zahl von auf dem Management Server registrierten Maschinen bequem schützen bzw. sichern zu können. Wählen Sie bei Erstellung eines zentralen Backup-Plans eine Gruppe und der Plan wird daraufhin auf alle Maschinen dieser Gruppe bereitgestellt. Sobald eine neue Maschine in einer Gruppe erscheint, wird der zentrale Backup-Plan auch auf dieser Maschine bereitgestellt. Falls eine Maschine von einer Gruppe entfernt wird, wird auch der zentrale Backup-Plan von dieser Maschine entfernt. Eine einzelne Maschine kann Mitglied in mehr als einer Gruppe sein.

Standardgruppe

Sobald eine Maschine auf dem Management Server registriert wurde, erscheint Sie in der vorgegebenen Standardgruppe **Alle Maschinen mit Agenten**. Diese Gruppe existiert immer auf einem Management Server und kann weder bearbeitet noch gelöscht werden. Eine vorgegebene Standardgruppe kann keine verschachtelten Gruppen enthalten.

Um alle registrierten Maschinen auf einmal schützen bzw. sichern zu können, erstellen Sie einen zentralen Backup-Plan unter Wahl der Gruppe **Alle Maschinen mit Agenten**. Alle Maschinen mit einem einzigen Backup-Plan zu schützen ist jedoch üblicherweise nicht zufriedenstellend, da die

Maschinen unterschiedliche Aufgaben haben. Die zu sichernden Daten sind spezifisch für jede Abteilung, manche Daten müssen häufig erfasst werden, bei anderen erfolgt das Backup nur zweimal im Jahr. Von daher werden Sie vermutlich verschiedene Backup-Pläne für diverse Arten von Maschinen erstellen. In diesem Fall sollten Sie die Erstellung benutzerdefinierter Gruppen erwägen.

Benutzerdefinierte Gruppen

Benutzerdefinierte Gruppen werden vom Administrator des Management Servers erstellt. Das Erstellen von benutzerdefinierten Gruppen hilft dem Administrator, die Datensicherung nach Firmenabteilungen zu organisieren, z.B. nach Active Directory-Organisationseinheiten, verschiedenen Anwendergruppen, nach örtlichen Gesichtspunkten usw.

Eine benutzerdefinierte Gruppe kann eine oder mehrere verschachtelte Gruppen enthalten. Jede benutzerdefinierte Gruppe kann bearbeitet oder gelöscht werden. Der Administrator kann folgende benutzerdefinierte Gruppen erstellen:

- **Statische Gruppen**

  Die statischen Gruppen enthalten manuell vom Administrator hinzugefügte Maschinen. Der Inhalt einer statischen Gruppe ändert sich niemals, außer der Administrator fügt ihr expliziert eine Maschine hinzu oder löscht eine.

  Beispiel: Sie erstellen eine benutzerdefinierte Gruppe für die Buchhaltung und fügen die entsprechenden Maschinen der Gruppe manuell hinzu. Die Buchhaltungsmaschinen sind geschützt, sobald Sie den zentralen Backup-Plan für diese Gruppe erstellen. Wird ein neuer Buchhalter eingestellt, so müssen Sie die neue Maschine der Gruppe manuell hinzufügen.

- **Dynamische Gruppen**

  Die dynamischen Gruppen enthalten Maschinen, die auf Basis von durch den Administrator spezifizierten Kriterien automatisch hinzugefügt werden. Der Inhalt einer dynamischen Gruppe ändert sich automatisch. Eine Maschine verbleibt solange in der Gruppe, wie sie die spezifizierten Kriterien erfüllt.

  Beispiel: Die Buchhaltungsabteilung bildet eine eigene Active Directory-Organisationseinheit (Organizational Unit, OU). Sie spezifizieren einfach die OU der Buchhaltung als Mitgliedschaftskriterium für die Gruppe und erstellen für diese den zentralen Backup-Plan. Bei Einstellung eines neuen Buchhalters wird seine neue Maschine genau dann in die Gruppe aufgenommen, wenn sie auch zur Organisationseinheit (Organization Unit, OU) hinzugefügt wird – wodurch sie dann auch automatisch geschützt wird.

  Tipp. Um das Kriterium „Active Directory-Organisationseinheit“ optimal zu nutzen, sollten Sie erwägen, die Active Directory-Hierarchie im Management Server zu reproduzieren.

Zu weiteren Informationen über Aktionen mit Gruppen und Maschinen siehe die folgenden Abschnitte:

- Aktionen fьr Gruppen (S. 417)
- Aktionen mit Maschinen (S. 409)

15.4.2.2 Aktionen mit Maschinen

Maschinen auf dem Management Server registrieren

Sobald eine Maschine zur Gruppe **Alle Maschinen mit Agenten** hinzugefügt oder importiert wurde, wird sie auch auf dem Management Server registriert. Registrierte Maschinen sind für das Deployment zentraler Backup-Pläne sowie die Durchführung anderer zentraler Verwaltungsaktionen verfügbar. Die Registrierung stellt eine Vertrauensstellung (Trusted Relationship) zwischen dem Agenten auf der Maschine und dem Management Server her.

Aktionen zum Hinzufügen und Importieren sind verfügbar, wenn Sie die Ansicht **Maschinen mit Agenten** oder die Gruppe **Alle Maschinen mit Agenten** im Navigationsbaum auswählen.

Aufgabe	Lösung
Eine neue Maschine zum Management Server hinzufügen	Klicken Sie auf **Maschine zum AMS hinzufügen**. Wählen Sie im Fenster **Maschine hinzufügen** (S. 412) die Maschine aus, die dem Management Server hinzugefügt werden soll.
Mehrere Maschinen hinzufügen	Klicken Sie auf **Mehrere Maschinen hinzufügen**. Spezifizieren Sie die Maschinen, die dem Management Server hinzugefügt werden sollen. Auf diese Art können Sie Maschinen hinzufügen, auf den Windows ohne einen installierten Agenten läuft. Der Agent für Windows wird automatisch durch Verwendung der Remote-Installationsfunktion hinzugefügt. Sie Details siehe den Abschnitt '"Die Liste der Maschinen spezifizieren' in der Installationsanleitung.
Maschinen mit einer Liste in der Textdatei synchronisieren	Klicken Sie auf **Mit Datei synchronisieren**. Spezifizieren Sie eine Textdatei mit der Liste der Maschinen. Nach der Synchronisierung verbleiben nur die in der Datei aufgelisteten Maschinen auf dem Management Server registriert. Zu Details siehe 'Synchronisieren von Maschinen mit einer Textdatei (S. 413)'.

Die Verwaltungskonsole spricht den Agenten an und löst die Registrierung aus. Da für die Registrierung die Teilnahme des Agenten erforderlich ist, kann diese Aktion nicht ausgeführt werden, wenn die Maschine offline ist.

Ein weiterer Agent, der auf einer registrierten Maschine registriert wird, wird automatisch auch auf demselben Management Server registriert. Mehrere Agenten werden gemeinsam registriert und deregistriert.

Löschen der ausgewählten Maschine vom Management Server

Aufgabe	Lösung
Eine Maschine vom Management Server löschen	Klicken Sie auf **Maschine vom AMS löschen**. Daraufhin werden die Backup-Pläne entfernt und die Verknüpfungen zu zentralen Depots von der Maschine gelöscht. Ist die Maschine derzeit nicht verfügbar, dann werden die Aktionen mit der Maschine ausgeführt, sobald diese für den Management Server wieder verfügbar ist.

Gruppierungsaktionen

Aufgabe	Lösung
Eine benutzerdefinierte statische oder dynamische Gruppe erstellen	Klicken Sie auf **Gruppe erstellen**. Geben Sie im Fenster **Gruppe erstellen** (S. 418) die erforderlichen Parameter für die Gruppe an. Die neue Gruppe wird in der Gruppe erstellt, in der die Maschine Mitglied ist (mit Ausnahme der Standardgruppe **Alle Maschinen mit Agenten**).
Eine Maschine einer anderen statischen Gruppe hinzufügen	Klicken Sie auf **Zu anderer Gruppe hinzufügen**. Geben Sie im Fenster **Zu Gruppe hinzufügen** (S. 414) die Gruppe an, in die die ausgewählte Maschine kopiert werden soll. Die zentralen Backup-Pläne der Gruppen, deren Mitglied die Maschine ist, werden auf die Maschine bereitgestellt.

Aufgabe	Lösung
Für Maschinen in benutzerdefinierten Gruppen	
Maschinen zu einer statischen Gruppe hinzufügen	Klicken Sie auf **Maschinen zu Gruppe hinzufügen**. Wählen Sie im Fenster **Maschinen zu Gruppe hinzufügen** (S. 414) die Maschinen, die Sie hinzufügen wollen. Die zentralen Backup-Pläne dieser Gruppe werden auf die ausgewählten Maschinen bereitgestellt.
Eine Maschine in eine andere statische Gruppe verschieben	Klicken Sie auf **Verschieben zu Gruppe**. Wählen Sie im Fenster **Verschieben zu Gruppe** (S. 414) die Gruppe aus, in die die Maschine verschoben werden soll. Alle zentralen Backup-Pläne der Gruppe, in der die Maschine zuvor war, werden entfernt. Die zentralen Backup-Pläne der Gruppe, deren Mitglied die Maschine jetzt ist, werden auf die Maschine bereitgestellt.
Eine Maschine aus der aktuellen statischen Gruppe entfernen	Klicken Sie auf **Entfernen von Gruppe**. Die zentralen Backup-Pläne der Gruppe werden automatisch von der Maschine entfernt.

Direkte Verwaltung

Aufgabe	Lösung
Einen Backup-Plan auf einer Maschine erstellen	Klicken Sie auf **Backup**. Diese Aktion wird ausführlich im Abschnitt 'Einen Backup-Plan erstellen (S. 58)' beschrieben.
Daten wiederherstellen	Klicken Sie auf **Recovery**. Diese Aktion wird ausführlich im Abschnitt 'Daten wiederherstellen (S. 146)' beschrieben.
Mit einer Maschine direkt verbinden	Klicken Sie auf **Direkt verbinden.** Stellt eine direkte Verbindung mit der verwalteten Maschine her. Ermöglicht die Administrierung einer verwalteten Maschine und die Ausführung aller direkten Verwaltungsaktionen (S. 489).

Andere Aktionen

Aufgabe	Lösung
Detaillierte Informationen zu einer Maschine anzeigen	Klicken Sie auf **Details**. Überprüfen Sie im Fenster **Maschinendetails** (S. 415) die Informationen zur Maschine.
Log-Einträge einer Maschine anzeigen	Klicken Sie auf **Log**. Die Ansicht **Log** (S. 435) wird mit einer Liste der Log-Einträge für die Maschine angezeigt.
Update der Lizenz eines Agenten auf einer Maschine	Klicken Sie auf **Lizenz wechseln**. Gründe zum Wechseln einer Lizenz (S. 375) beinhalten: ▪ Vom Testmodus zur Vollversion umstellen. ▪ Aktivierung von Acronis Deduplication. ▪ Aktivierung von Acronis Universal Restore.

Aufgabe	Lösung
Update aller Maschinen-bezogenen Informationen	Klicken Sie auf **Synchronisieren**. Der Management Server schickt eine Anfrage an die Maschine und aktualisiert die Datenbank mit den neuesten Informationen. Die Liste der virtuellen Maschinen wird zusammen mit der Synchronisierung automatisch aktualisiert.
Eine Liste von Maschinen aktualisieren	Klicken Sie auf **Aktualisieren**. Die Verwaltungskonsole aktualisiert die Liste der Maschinen vom Management Server mit den neuesten Informationen. Obwohl die Liste der Maschinen auf der Basis von Ereignissen automatisch aktualisiert wird, kann es sein, dass die Daten aufgrund einer gewissen Verzögerung nicht augenblicklich vom Management Server abgerufen werden. Eine manuelle Aktualisierung garantiert daher, dass auch wirklich die allerneuesten Daten angezeigt werden.

Eine Maschine dem Management Server hinzufügen

Um zentrale Backup-Pläne vom Acronis Backup & Recovery 11.5 Management Server auf einer verwalteten Maschine bereitstellen und andere zentrale Verwaltungsaktionen ausführen zu können, müssen Sie die Maschine auf dem Management Server registrieren.

Registrierung auf der Seite des Management Servers auslösen

So fügen Sie eine Maschine hinzu

1. Wählen Sie im Verzeichnisbaum **Navigation** den Eintrag **Maschinen mit Agenten**.
2. Klicken Sie in der Symbolleiste auf **Maschine zum AMS hinzufügen**.
3. Geben Sie im Feld **IP/Name** den Namen oder die IP-Adresse der Maschine ein oder klicken Sie auf **Durchsuchen...** und suchen Sie im Netzwerk nach der Maschine.

   Hinweis für Benutzer der Virtual Edition: *Wenn Sie einen VMware ESX(i)-Host hinzufügen, geben Sie die IP der virtuellen Appliance oder von der Windows-Maschine an, auf der der Acronis Backup & Recovery 11.5 Agent für ESX(i) läuft.*

4. Spezifizieren Sie die Anmeldedaten eines Kontos, welches auf der Maschine über administrative Berechtigungen verfügt.

   Wenn Sie eine unter Windows Vista (oder höher) laufende Maschine hinzufügen, die *kein* Mitglied einer Active Directory-Domain ist, müssen Sie entweder das integrierte Administrator-Konto spezifizieren oder die Benutzerkontensteuerung (UAC) (S. 388) auf der Maschine deaktivieren.

   Hinweis für Benutzer der Virtual Edition: *Wenn Sie einen VMware ESX(i)-Host hinzufügen, dann spezifizieren Sie den Benutzernamen und das Kennwort für Ihren vCenter-Server oder ESX(i)-Host.*

   - **Benutzername**. Achten Sie bei Eingabe des Namens eines Benutzerkontos für Active Directory darauf, auch den Domain-Namen anzugeben (Domain\Benutzername).
   - **Kennwort**. Das Kennwort für das Konto.
5. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Maschinenseitige Registrierung auslösen

Die Registrierung kann auch maschinenseitig ausgelöst werden.

1. Verbinden Sie die Konsole mit der Maschine, auf der Acronis Backup & Recovery 11.5 Agent installiert ist. Wenn Sie zur Eingabe von Anmeldedaten aufgefordert werden, dann spezifizieren Sie die Anmeldedaten eines Mitglieds der Gruppe der **Administratoren** auf dieser Maschine.

2. Wählen Sie aus dem Menü **Optionen** –> Die Befehle **Maschinen-Optionen** –> **Verwaltung der Maschine**.
3. Wählen Sie **Zentrale Verwaltung** und spezifizieren Sie den Management Server, auf dem die Maschine registriert werden soll. Siehe "Verwaltung der Machine (S. 383)" für Details.

Synchronisieren von Maschinen mit einer Textdatei

Während der Synchronisierung passt der Management Server die Gruppe **Alle Maschinen mit Agenten** an, in Übereinstimmung mit der als .txt- oder .csv-Datei zur Verfügung gestellten Maschinenliste. Der Management Server:

- Fügt Maschinen aus der Liste hinzu, die nicht registriert sind
- Löscht registrierte Maschinen, die nicht in der Liste enthalten sind
- Löscht registrierte Maschinen aus der Liste, deren derzeitige Verfьgbarkeit (S. 415) als **Zurückgezogen** angegeben ist, und versucht, sie erneut hinzuzufügen.

Als Ergebnis befinden sich nur noch solche Maschinen in der Gruppe **Alle Maschinen mit Agenten**, die in der Datei aufgelistet sind.

Anforderungen für die Textdatei

In der Datei sollte eine Maschine pro Zeile jeweils mit ihrem Namen oder ihrer IP-Adresse aufgeführt sein.

Beispiel:

```
Machine_name_1
Machine_name_2
192.168.1.14
192.168.1.15
```

Hat die spezifizierte Datei keinen Inhalt, dann werden alle Maschinen mit Agenten vom Management Server gelöscht.

Eine registrierte Maschine muss über ihre Registrierungsadresse spezifiziert werden: Was bedeutet, dass Sie exakt denselben Host-Namen, den 'Fully Qualified Domain Name' (FQDN) oder die IP-Adresse angeben müssen, die verwendet wurden, als die Maschine ursprünglich dem Management Server hinzugefügt wurde. Anderenfalls wird die Maschine gelöscht und erneut so hinzugefügt, als wäre sie eine andere Maschine. Das bedeutet, dass alle zentralen Backup-Pläne, egal ob geerbt oder direkt bereitgestellt, von der Maschine entfernt werden und dass ihre Mitgliedschaft in der statischen Gruppe verloren geht.

Die Registrierungsadresse einer Maschine kann in der Spalte **Registrierungsadresse** in jeder Management Server-Ansicht gefunden werden, in der die Maschine enthalten ist (standardmäßig ist die Spalte versteckt).

Um Diskrepanzen zu vermeiden, können Sie die Maschinen zu Anfang von einer Textdatei importieren. Modifizieren Sie nach Bedarf diese Datei später durch Hinzufügen oder Entfernen von Maschinen – aber ändern Sie nicht die Namen bzw. Adressen der Maschinen, die registriert bleiben müssen.

So synchronisieren Sie Maschinen mit einer Textdatei

1. Wählen Sie im Verzeichnisbaum **Navigation** entweder **Maschinen mit Agenten** oder **Alle Maschinen mit Agenten**.
2. Klicken Sie in der Symbolleiste auf **Mit Datei synchronisieren**.
3. Geben Sie im Feld **Pfad** einen Pfad zu der .txt- oder .csv-Datei ein oder klicken Sie auf **Durchsuchen** und wählen Sie dann im Fenster **Durchsuchen** die Datei aus.

4. Geben Sie unter **Anmeldeeinstellungen** Namen und Kennwort eines Benutzers ein, der Mitglied der Gruppe Administratoren für alle in der Datei aufgelisteten Maschinen ist.
5. Klicken Sie auf **OK**, um den Importvorgang zu starten.

Befehlszeilenwerkzeug zur Synchronisation

Der Acronis Backup & Recovery 11.5 Management Server verfügt über ein Befehlszeilenwerkzeug, mit dem Sie eine Batch-Datei erstellen können, um den Synchronisationstask unter Verwendung des Windows Scheduler zu planen.

So synchronisieren Sie Maschinen mit einer Textdatei unter Verwendung der Befehlzeile

1. Melden Sie sich als ein Mitglied der Sicherheitsgruppe **Acronis Centralized Admins** an.
2. Wechseln Sie in der Eingabeaufforderung zu dem Ordner, wo der Acronis Backup & Recovery 11.5 Management Server installiert wurde – standardmäßig ist das: **C:\Programme\Acronis\AMS**.
3. Führen Sie folgenden Befehl aus:

```
syncmachines [path_to_the_file] {username password}
```

   wobei:

   - [Pfad_zur_Datei] der Pfad zu einer .txt- oder .csv-Datei ist, die die Liste der Maschinen enthält. Das Befehlszeilenwerkzeug akzeptiert keine Leerzeichen in der Pfadbezeichnung.
   - {username password} (Benutzername Kennwort) gehört zu einem Benutzer, der auf allen in der Datei gelisteten Maschinen ein Mitglied der Gruppe 'Administratoren' ist. Wenn nichts angegeben, wird der „Single Sign-on“-Mechanismus verwendet, um auf allen Maschinen Aktionen auszuführen.

Eine Maschine einer anderen Gruppe hinzufügen

So fügen Sie die ausgewählte Maschine einer anderen Gruppe hinzu

1. Wählen Sie die Gruppe aus, der die Maschine hinzugefügt werden soll.
2. Klicken Sie auf **OK**.

Die hinzugefügte Maschine wird Mitglied von mehr als einer Gruppe. Als Ergebnis verbleiben die zentralen Backup-Pläne für die erste Gruppe auf der Maschine und werden auch die zentralen Backup-Pläne für die zweite, dritte usw. Gruppe auf die Maschine bereitgestellt.

Eine Maschine in eine andere Gruppe verschieben

So verschieben Sie die ausgewählte Maschine in eine andere Gruppe

1. Wählen Sie in der Gruppenstruktur die Gruppe aus, in die die Maschine verschoben werden soll.
2. Klicken Sie auf **OK**.

Die zu verschiebende Maschine verlässt eine Gruppe und wird Mitglied einer anderen Gruppe. Als Ergebnis werden die für die erste Gruppe erstellten zentralen Backup-Pläne von der Maschine entfernt und die für die zweite Gruppe erstellten zentralen Backup-Pläne auf der Maschine bereitgestellt.

Maschinen zu einer Gruppe hinzufügen

So fügen Sie der ausgewählten Gruppe Maschinen hinzu

1. Wählen Sie aus dem Verzeichnisbaum der Gruppen diejenige Gruppe aus, deren Maschinen hinzugefügt werden sollen.
2. Wählen Sie im rechten Teil des Fensters die Maschinen aus.

3. Um weitere Maschinen aus anderen Gruppen hinzuzufügen, wiederholen Sie für jede dieser Gruppen die Schritte 1 und 2.
4. Klicken Sie auf **OK**, um die Maschinen hinzuzufügen.

Sobald die Maschinen in der Gruppe erscheinen, werden die für die Gruppe erstellten zentralen Backup-Pläne (sofern vorhanden) auf die Maschinen bereitgestellt. Wenn eine der ausgewählten Maschinen nicht verfügbar oder aktuell nicht erreichbar ist, wird die Aktion im Management Server als „Ausstehend“ abgelegt und sie wird ausgeführt, sobald die Maschine für den Server wieder verfügbar ist.

Maschinendetails

Vier Registerlaschen sammeln alle Informationen über eine ausgewählte Maschine und ermöglichen dem Administrator des Management Servers Aktionen auf die Backup-Pläne und Tasks dieser Maschine anzuwenden.

Maschine

Auf dieser Registerkarte werden folgende Informationen über registrierte Maschinen angezeigt:

- **Name** – Name der ausgewählten Maschine (wird vom **Computernamen** in Windows bezogen).
- **Registrierungsadresse** – Computername oder IP-Adresse der gewählten Maschine. Der Administrator des Management Servers kann während der Registrierung einer Maschine (S. 494) dieser einen Namen oder eine IP-Adresse zuweisen, um die Maschine auf dem Management Server zu identifizieren.
- **IP-Adresse** – IP-Adresse der ausgewählten Maschine.
- **Laufwerkszustandseinstufung** – das Stadium des Laufwerkszustandes der Maschine. Dieses Feld ist mit **Nicht verfügbar** eingestellt, falls das Utility 'Acronis Drive Monitor' nicht auf der Maschine installiert ist. Der Acronis Drive Monitor prüft automatisch auf Laufwerksprobleme und trifft Vorhersagen, wann ein Laufwerk möglicherweise ausfällt. Sie können das kostenlose Utility unter http://www.acronis.de herunterladen.
- **Status** – der Schutzstatus der Maschine. Dies entspricht dem Ergebnis des letztens Backups der Daten der Maschine. Die Ergebnisse anderer Aktionen (wie Validierung, Bereinigung oder Replikation) haben keinen Einfluss auf den Status. Mögliche Statuswerte sind **OK**, **Warnung** und **Fehler**.
- **Letzte Verbindung** – Zeit, die vergangen ist, seit der Management Server das letzte Mal mit der Maschine verbunden war.
- **Letztes erfolgreiches Backup** – Zeit, die seit dem letzten erfolgreichen Backup vergangen ist.
- **Nächstes Backup** – wie viel Zeit bis zum nächsten Backup verbleibt.
- **Verfügbarkeit:**
  - **Online** – Maschine ist für den Management Server verfügbar. Das bedeutet, dass die letzte Verbindung des Management Servers mit der Maschine erfolgreich war. Die Verbindung wird alle 2 Minuten aufgebaut.
  - **Offline** – Maschine ist für den Management Server nicht verfügbar. Sie ist ausgeschaltet oder das Netzwerkkabel ist nicht angeschlossen.
  - **Unbekannt** – dieses Stadium besteht nach dem Hinzufügen der Maschine so lange, bis zum ersten Mal eine Verbindung zwischen dem Management Server und der Maschine hergestellt wird oder bis der Dienst des Management Servers gestartet wird.
  - **Zurückgezogen** – Die Maschine wurde auf einem anderen Management Server registriert oder der Parameter **Autonome Verwaltung** war auf der Maschine im Bereich **Optionen** –>

Maschinen-Optionen –> **Verwaltung der Maschine** (S. 383) ausgewählt. In diesem Fall ist es nicht möglich, die Maschine über den aktuellen Management Server zu steuern. Um die Kontrolle über die Maschine zurückzugewinnen, müssen Sie diese vom aktuellen Management Server erst entfernen – und dann die Maschine wieder neu hinzufügen.

  - **Abgelaufen** – für den Agenten der Maschine ist der Testzeitraum abgelaufen. Um einen Lizenzschlüssel für den Agenten zu spezifizieren, können Sie mit der rechten Maustaste auf die Maschine klicken. Klicken Sie anschließend auf den Befehl **Lizenz wechseln** (S. 375).
- **Installierte Agenten** – Namen der Acronis-Agenten, die auf der Maschine installiert sind.
- **Betriebssystem** – Betriebssystem, unter dem der Agent der Maschine ausgeführt wird.
- **Prozessor** – der in der verwaltenden Maschine verwendete CPU-Typ.
- **CPU-Takt** – Taktrate der CPU.
- **RAM** – Hauptspeichergröße.
- **Kommentar** – Beschreibung der Maschine (wird von der **Computerbeschreibung** in Windows bezogen).

Backup-Pläne und Tasks

Zeigt eine Liste der (lokalen und zentralen) Pläne sowie der Tasks an, die auf der ausgewählten Maschine vorhanden sind.

Aktionen

Für eine Liste von Aktion, die für die Backup-Pläne und Tasks einer Maschine verfügbar sind, siehe den Abschnitt 'Aktionen fьr Backup-Plдne und Tasks (S. 361)'.

Filtern und Sortieren

Das Filtern und Sortieren von Backup-Plänen und Tasks erfolgt wie im Abschnitt 'Tabellenelemente sortieren, filtern und konfigurieren (S. 29)' beschrieben.

Mitglied von

Diese Registerkarte wird nur angezeigt, wenn die ausgewählte Maschine Mitglied einer oder mehrerer benutzerdefinierter Gruppen ist. Auf der Registerkarte wird eine Liste der Gruppen angezeigt, in denen die Maschine Mitglied ist.

Aktionen

Aktion	Lösung
Details einer Gruppe anzeigen	Klicken Sie auf **Details**. Sie gelangen zum Fenster **Group details**, wo Sie alle auf diese Gruppe bezogenen Informationen überprüfen können.
Eine Maschine aus einer Gruppe entfernen.	Klicken Sie auf **Aus dieser Gruppe entfernen**. Die zentralen Pläne, die an die übergeordnete Gruppe verteilt wurden, wirken sich nicht länger auf diese Maschine aus.
Eine Liste von Gruppen aktualisieren	Klicken Sie auf **Aktualisieren**. Gruppen können, während Sie eine Maschine einsehen, hinzugefügt, gelöscht oder modifiziert werden. Klicken Sie auf **Aktualisieren**, um die Informationen über die Gruppen mit den neuesten Änderungen zu aktualisieren. Dies öffnet die Ansicht **Log** mit vorgefilterten Log-Einträgen für die ausgewählte Gruppe.

Fortschritt

In der Registerlasche **Fortschritt** werden alle aktuell laufenden Aktivitäten und Tasks der gewählten Maschine angezeigt. Die Registerlasche bietet Informationen über den Fortschritt des Tasks, die verstrichene Zeit und andere Parameter.

Verwaltete virtuelle Maschinen

Auf diesem Reiter wird eine Liste der Maschinen angezeigt, die auf dem ausgewählten Virtualisierungsserver gehostet oder von der angegebenen virtuellen Appliance verwaltet werden.

Auf Basis dieser Liste von gehosteten, virtuellen Maschinen können Sie eine dynamische Gruppe erstellen. Klicken Sie dazu auf **Dynamische Gruppe erstellen**. Auf die erstellte Gruppe können Sie in der Virtuelle Maschinen-Ansicht zugreifen.

15.4.2.3 Aktionen mit Gruppen

Die Aktionen sind verfügbar, wenn Sie die Ansicht **Maschinen mit Agenten** im Verzeichnisbaum **Navigation** wählen. Sie wählen eine Gruppe aus dem Verzeichnisbaum **Navigation** oder in der Ansicht **Maschinen mit Agenten**, um mit dieser Gruppe eine Aktion durchzuführen.

Nachfolgend finden Sie eine Anleitung zur Ausführung von Aktionen auf ausgewählte Gruppen.

Aufgabe	Lösung
Eine Maschine dem Management Server hinzufügen	Diese Aktion ist nur in der Ansicht **Maschinen mit Agenten** und für die Gruppe **Alle Maschinen mit Agenten** aktiviert. Klicken Sie auf **Maschine zum AMS hinzufügen**. Wählen Sie im Fenster **Maschine hinzufügen** (S. 412) die Maschine aus, die dem Management Server hinzugefügt werden soll.
Maschinen mit einer Liste in der Textdatei synchronisieren	Diese Aktion ist nur in der Ansicht **Maschinen mit Agenten** und für die Gruppe **Alle Maschinen mit Agenten** aktiviert. Klicken Sie auf **Mit Datei synchronisieren**. Spezifizieren Sie eine Textdatei mit der Liste der Maschinen. Nach der Synchronisierung verbleiben nur die in der Datei aufgelisteten Maschinen auf dem Management Server registriert. Zu weiteren Informationen siehe '**Synchronisieren von Maschinen mit einer Textdatei** (S. 413)'.
Eine benutzerdefinierte statische oder dynamische Gruppe erstellen	Klicken Sie auf **Gruppe erstellen**. Geben Sie im Fenster **Gruppe erstellen** (S. 418) die erforderlichen Parameter für die Gruppe an. Benutzerdefinierte Gruppen können im Stammverzeichnis (**Maschinen mit Agenten**) oder in anderen benutzerdefinierten Gruppen erstellt werden.
Maschinen zur ausgewählten statischen Gruppe hinzufügen	Klicken Sie auf **Maschinen zu Gruppe hinzufügen**. Wählen Sie im Fenster **Maschinen zu Gruppe hinzufügen** (S. 414) die Maschinen aus, die hinzugefügt werden sollen. Nicht anwendbar auf dynamische Gruppen.

Aufgabe	Lösung
Einen neuen Backup-Plan für eine Gruppe erstellen	Klicken Sie auf **Backup-Plan erstellen**, um einen Backup-Plan für die ausgewählte Gruppe zu erstellen. Diese Aktion wird ausführlich im Abschnitt 'Einen Backup-Plan erstellen (S. 58)' beschrieben.
Detaillierte Informationen zu einer Gruppe anzeigen	Klicken Sie auf **Details**. Überprüfen Sie im Fenster **Gruppendetails** (S. 421) die Informationen zur ausgewählten Gruppe.
Eine benutzerdefinierte Gruppe/Untergruppe umbenennen	Klicken Sie auf **Umbenennen**. Geben Sie in der Spalte **Name** einen neuen Namen für die ausgewählte Gruppe ein. Standardgruppen können nicht umbenannt werden.
Eine benutzerdefinierte Gruppe bearbeiten	Klicken Sie auf **Bearbeiten**. Ändern Sie im Fenster **Gruppe bearbeiten** (S. 421) die erforderlichen Parameter für die Gruppe.
Eine benutzerdefinierte Gruppe in eine andere verschieben	Klicken Sie auf **Verschieben nach**. Geben Sie im Fenster **Verschieben zu Gruppe** (S. 420) eine Gruppe an, die die neue übergeordnete Gruppe für die ausgewählte Gruppe wird.
Eine benutzerdefinierte Gruppe löschen	Klicken Sie auf **Löschen**. Beim Löschen einer übergeordneten Gruppe werden auch deren Untergruppen gelöscht. Zentrale Backup-Pläne, für die übergeordnete Gruppe erstellt und von den Untergruppen übernommen, werden von allen Mitgliedern der gelöschten Gruppen entfernt. Backup-Pläne, die direkt für die Mitglieder erstellt wurden, bleiben erhalten.
Eine Liste von Gruppen aktualisieren	Klicken Sie auf **Aktualisieren**. Die Management Konsole aktualisiert die Liste der Gruppen vom Management Server mit den neuesten Informationen. Obwohl die Liste der Gruppen auf der Basis von Ereignissen automatisch aktualisiert wird, kann es sein, dass die Daten aufgrund einer gewissen Verzögerung nicht augenblicklich vom Management Server abgerufen werden. Eine manuelle Aktualisierung garantiert daher, dass auch die allerneuesten Daten angezeigt werden.

Eine benutzerdefinierte statische oder dynamische Gruppe erstellen

So erstellen Sie eine Gruppe

1. Geben Sie im Feld **Name** die Bezeichnung für die zu erstellende Gruppe ein.
2. Wählen Sie den Typ der Gruppe:
   a. **Statisch** – zum Erstellen einer Gruppe, die Maschinen enthält, die manuell hinzugefügt werden.
   b. **Dynamisch** – zum Erstellen einer Gruppe, die Maschinen enthält, die nach definierten Kriterien automatisch hinzugefügt werden.

      Klicken Sie auf **Kriterium hinzufügen** und wählen Sie das Kriterienmuster aus.

      - **Betriebssystem**

Alle Maschinen, auf denen das ausgewählte Betriebssystem läuft, werden zu Mitgliedern der dynamischen Gruppe.

- **Organisationseinheit** (S. 419)

  Alle Maschinen, die zur angegebenen Organisationseinheit gehören, werden zu Mitgliedern der dynamischen Gruppe.

- **IP-Adressbereich**

  Alle Maschinen, deren IP-Adressen im angegeben IP-Bereich liegen, werden zu Mitgliedern der dynamischen Gruppe.

- **In txt/csv-Datei aufgelistet** (S. 420)

  Alle Maschinen, die in der angegebenen .txt- oder .csv-Datei aufgelistet sind, werden zu Mitgliedern der dynamischen Gruppe.

3. Geben Sie im Feld **Gruppenbeschreibung** eine Erläuterung für die erstellte Gruppe ein.
4. Klicken Sie auf **OK**.

Mehrere Kriterien hinzufügen

Durch das Hinzufügen mehrerer Kriterien wird ein Zustand entsprechend folgender Regeln geschaffen:

a) Alle Einträge des gleichen Kriteriums werden durch logische Addition (ODER) miteinander verknüpft.

Z.B. werden durch die Kriterienmenge

Betriebssystem: Windows Server 2003

Betriebssystem: Windows Server 2008

alle Maschinen derselben Gruppe hinzugefügt, auf denen der Windows Server 2003 oder der Windows Server 2008 als Betriebssystem ausgeführt wird.

b) Einträge für unterschiedliche Kriterien werden durch logische Multiplikation (UND) miteinander verknüpft

Erwägen Sie beispielsweise folgende Kriterienzusammenstellung:

Betriebssystem: Windows Server 2003

Betriebssystem: Windows Server 2008

Organisationseinheit: SERVER

IP-Bereich: 192.168.17.0 - 192.168.17.55

Diese Kriterien fügen alle Maschinen derselben Gruppe hinzu, auf denen das Betriebssystem Windows 2003 oder Windows 2008 ausgeführt wird, die aber außerdem zur Organisationseinheit SERVER gehören und deren IP-Adressen im Bereich 192.168.17.0 – 192.168.17.55 liegen.

Kriterium „Organisationseinheit“

Das Kriterium „Organisationseinheit“ wird für die Domain, zu der der Management Server aktuell gehört, wie folgt spezifiziert: *OU=OU1*

Wählen Sie eine organisatorische Einheit im Active Directory durch einen Klick auf **Durchsuchen** oder durch manuelle Eingabe. Wenn die Anmeldedaten für die Domänen in den Optionen des Management Servers nicht angegeben wurden, wird das Programm danach fragen. Die Anmeldedaten werden unter Domдnen-Zugriffsberechtigungen (S. 439) gespeichert.

Ein Beispiel: Angenommen, die Domain *us.corp.example.com* hat OU1 (befindet sich im Stammverzeichnis), OU1 hat OU2 und OU2 hat OU3. Und Sie müssen die Maschinen von OU3 hinzufügen. Das Kriterium wird daher sein: *OU=OU3, OU=OU2, OU=OU1*

Falls OU3 „Child Container" hat und Sie die Maschinen dieser Container ebenfalls der Gruppe hinzufügen müssen, dann aktivieren Sie das Kontrollkästchen **Child Container einschließen**.

Kriterium 'In txt/csv-Datei aufgelistet'

Wenn Sie dieses Kriterium verwenden, beinhaltet die dynamische Gruppe die in der .txt- oder .csv-Datei aufgelisteten Maschinen.

Wenn Sie die Datei später verändern, ändert sich der Inhalt der Gruppe entsprechend. Die Datei wird alle 15 Minuten geprüft.

Wenn Sie die Datei später löschen, oder sie nicht mehr verfügbar ist, entspricht der Inhalt der Gruppe der letzten Version der Liste, die in der Datei gespeichert war.

Anforderungen für die Textdatei

In der Datei sollte eine Maschine pro Zeile jeweils mit ihrem Namen oder ihrer IP-Adresse aufgeführt sein.

Beispiel:

```
Maschinenname_1
Maschinenname_2
192.168.1.14
192.168.1.15
```

Eine registrierte Maschine muss über ihre Registrierungsadresse spezifiziert werden, was bedeutet, dass Sie exakt denselben Host-Namen, den 'Fully Qualified Domain Name' (FQDN) oder die IP-Adresse angeben müssen, die verwendet wurden, als die Maschine ursprünglich dem Management Server hinzugefügt wurde. Anderenfalls wird die Maschine der Gruppe nicht hinzugefügt. Die Registrierungsadresse einer Maschine kann in der Spalte **Registrierungsadresse** in jeder Management Server-Ansicht gefunden werden, in der die Maschine enthalten ist (standardmäßig ist die Spalte versteckt).

Eine Gruppe in eine andere verschieben

So verschieben Sie die ausgewählte Gruppe in eine andere Gruppe oder in den Stammordner

1. Klicken Sie in der Gruppenstruktur auf die Gruppe, in die die ausgewählte Gruppe verschoben werden soll. Sie können eine beliebige benutzerdefinierte Gruppe (statisch oder dynamisch) in eine andere benutzerdefinierte Gruppe eines beliebigen Typs oder in den Stammordner verschieben.

   Der Stammordner des Maschinenverzeichnisbaums enthält *Gruppen der ersten Ebene*. Gruppen, die andere Gruppen enthalten, werden *übergeordnete Gruppen* genannt. Gruppen, die sich in übergeordneten Gruppen befinden, werden *Untergruppen* genannt. Alle zentralen, für die übergeordnete Gruppe erstellten Backup-Pläne werden ebenso auf die Maschinen ihrer untergeordneten Gruppen bereitgestellt.
2. Klicken Sie auf **OK**.

Benutzerdefinierte Gruppen bearbeiten

Die Bearbeitung einer benutzerdefinierten Gruppe wird auf die gleiche Weise ausgeführt wie die Erstellung (S. 418).

Die Änderung des Typs einer Gruppe führt dazu, dass diese konvertiert wird. Jede benutzerdefinierte Gruppe kann in eine dynamische Gruppe konvertiert werden, wenn sie vorher statisch war, und umgekehrt.

- Geben Sie bei der Konvertierung einer statischen Gruppe in eine dynamische Gruppe die Gruppierungskriterien an. Alle Mitglieder in der statischen Gruppe, die die angegebenen Kriterien nicht erfüllen, werden aus der dynamischen Gruppe entfernt.
- Für die Konvertierung einer dynamischen Gruppe in eine statische Gruppe sind zwei Optionen verfügbar – Sie können entweder den aktuellen Inhalt der Gruppe beibehalten oder die Gruppe leeren.

Gruppendetails

Fasst alle Informationen zur ausgewählten Gruppe auf zwei Registerkarten zusammen. Das ermöglicht die Durchführung von Aktionen mit den zentralen Backup-Plänen für eine Gruppe.

Gruppe

Zeigt die folgenden Informationen über die Gruppe:

- **Name** – Name der ausgewählten Gruppe
- **Übergeordnete Gruppe** (nur für Untergruppen) – Name der übergeordneten Gruppe
- **Maschinen** – Zahl der Maschinen in der Gruppe
- **Typ** – Typ der Gruppe (statisch oder dynamisch)
- **Kriterien** (nur für dynamische Gruppen) – Gruppierungskriterien
- **Beschreibung** – die Gruppenbeschreibung (falls spezifiziert)

Backup-Pläne

Zeigt eine Liste der zentralen Backup-Pläne an, die sich auf die Gruppe beziehen und ermöglicht die Ausführung folgender Aktionen:

Aktion	Lösung
Details eines Backup-Plans anzeigen	Klicken Sie auf **Details**. Überprüfen Sie im Fenster Backup-Plдne und Tasks alle Informationen, die sich auf den ausgewählten Backup-Plan beziehen.
Log eines Backup-Plans anzeigen	Klicken Sie auf **Log**. Die Ansicht **Log** zeigt eine Liste der Log-Einträge an, die sich auf den ausgewählten Backup-Plan beziehen.
Einen Backup-Plan ausführen	1. Klicken Sie auf **Ausführen**. 2. Wählen Sie aus dem Listenfeld den Task des Plans aus, den Sie ausführen müssen. Die Ausführung eines Backup-Plans startet auch unmittelbar den dazugehörigen, ausgewählten Task, ungeachtet seiner Planung und der Bedingungen auf den Maschinen, wohin der Plan bereitgestellt wird. Ein zentraler Backup-Plan kann nicht manuell ausgeführt werden, falls auf mindestens einer der im Plan enthaltenen Maschinen ein Agent von Acronis Backup & Recovery 10 läuft.

Aktion	Lösung
Einen Backup-Plan stoppen	Klicken Sie auf **Stopp**. Wenn Sie einen laufenden Backup-Plan stoppen, werden auch all seine Tasks auf allen Maschinen gestoppt, auf denen der Plan bereitgestellt wurde. Daher werden alle Task-Aktionen abgebrochen. Ein zentraler Backup-Plan kann nicht manuell gestoppt werden, falls auf mindestens einer der im Plan enthaltenen Maschinen der Acronis Backup & Recovery 10 Agent läuft.
Tabelle aktualisieren	Klicken Sie auf **Aktualisieren**. Die Management Konsole wird die Liste der für die Maschinegruppe existierenden Backup-Pläne mit den neuesten Informationen aktualisieren. Die Liste wird auf der Basis von Ereignissen automatisch aktualisiert. Möglicherweise werden die Daten dabei jedoch infolge einer gewissen Latenz nicht augenblicklich von der verwalteten Maschinengruppe abgerufen. Eine manuelle Aktualisierung garantiert daher, dass auch wirklich die allerneuesten Daten angezeigt werden.

Filtern und Sortieren

Das Filtern und Sortieren der Backup-Pläne und Tasks erfolgt auf gleiche Weise wie für die Ansicht **Backup-Pläne und Tasks**. Zu Details siehe Tabellenelemente sortieren, filtern und konfigurieren (S. 29).

15.4.3 Virtuelle Maschinen

Sie können virtuelle Maschinen unter Verwendung einer oder beider der folgenden Methoden zentral verwalten:

Hinzufügen einer virtuellen Maschine als physikalische Maschine

Installieren Sie den Agenten für Windows oder den Agenten für Linux in Acronis Backup & Recovery 11.5 auf der virtuellen Maschine und registrieren (S. 412) Sie ihn auf dem Management Server. Die virtuelle Maschine wird wie eine physikalische Maschine behandelt. Sie wird unter **Maschinen mit Agenten** in der Gruppe **Alle Maschinen mit Agenten** erscheinen.

Dieser Ansatz ist für folgende Situationen geeignet:

- Die Maschine wird nicht auf einem Virtualisierungsserver gehostet.
- Sie haben keine Lizenz für die Acronis Backup & Recovery 11.5 Virtual Edition.
- Die Virtual Edition unterstützt keine Backups auf Hypervisor-Ebene für dieses spezielle Virtualisierungsprodukt.
- Sie müssen Beschrдnkungen bei Backups auf Hypervisor-Ebene überwinden.

Hinzufügen einer virtuellen Maschine als virtuelle Maschine

Auf dem Acronis Backup & Recovery 11.5 Management Server wird eine Maschine als virtuell angesehen, wenn das Backup vom Virtualisierungshost erstellt werden kann, ohne dass ein Agent auf der Maschine installiert werden muss. Dies ist möglich, wenn Sie die Acronis Backup & Recovery 11.5 Advanced Server Virtual Edition verwenden.

Es gibt verschiedene Arten, wie Sie eine virtuelle Maschine zum Management Server hinzufügen können:

- Aktivieren Sie die Integration des Management Servers mit dem vCenter-Server.

Ergebnis: Die vom vCenter-Server verwalteten virtuellen Maschinen erscheinen unter **Virtuelle Maschinen** in der Gruppe **Alle virtuellen Maschinen**. Die Maschinen sehen wie unverwaltet aus (sind ausgegraut), können jedoch gesichert werden, falls während der Integration die Funktion zum automatischen Deployment des Agenten aktiviert wurde.

- Installieren und konfigurieren Sie den Agenten für ESX(i) VMware vSphere (Virtuelle Appliance) oder den Agenten für ESX(i) VMware vSphere (Windows). Registrieren Sie den Agenten auf dem Management Server.

  Ergebnis: Die Maschine mit dem Agenten (die virtuelle Appliance oder der Windows-Host) erscheint unter **Maschinen mit Agenten** in der Gruppe **Alle Maschinen mit Agenten**. Die vom Agenten verwalteten virtuellen Maschinen erscheinen unter **Virtuelle Maschinen** in der Gruppe **Alle virtuellen Maschinen**.

- Installieren Sie den Agenten fьr Hyper-V auf einem Hyper-V-Host oder auf allen Knoten eines Hyper-V-Clusters. Registrieren Sie den/die Agenten auf dem Management Server.

  Ergebnis: Der Hyper-V-Host (Knoten) erscheint unter **Maschinen mit Agenten** in der Gruppe **Alle Maschinen mit Agenten**. Die von dem/den Agenten verwalteten virtuellen Maschinen erscheinen unter **Virtuelle Maschinen** in der Gruppe **Alle virtuellen Maschinen**.

Virtuelle Maschinen, die zum Management Server als virtuelle Maschinen hinzugefügt wurden, sind im Verzeichnisbaum **Navigation** unter **Virtuelle Maschinen** präsent. Zu weiteren Informationen über die für diese Maschinen verfügbaren Aktionen siehe das Dokument 'Backups von virtuellen Maschinen'.

15.4.4 Backup-Pläne und Tasks

Die Ansicht **Backup-Pläne und Tasks** informiert Sie über die Datensicherung auf den Maschinen, die auf dem Management Server registriert sind. In dieser Ansicht werden die auf dem Management Server vorliegenden Backup-Pläne angezeigt – sowie die Tasks des Management Servers und der Storage Nodes.

Um überprüfen zu können, ob die Daten auf den Maschinen geschützt bzw. gesichert sind, auf denen der zentrale Plan bereitgestellt wurde, müssen Sie den kumulativen Status des Plans untersuchen.

Um herauszufinden, ob ein zentraler Backup-Plan momentan bereitgestellt, entfernt oder aktualisiert wird, müssen Sie das Verteilungsstadium des Plans überprüfen. In jedem der Stadien kann der Backup-Plan einen Status wie folgt haben: **Fehler**; **Warnung**; **OK**.

Um den aktuellen Fortschritt eines Tasks im Überblick zu behalten, verfolgen Sie sein Stadium (S. 365). Prüfen Sie den Status (S. 365) eines Tasks, um sein Ergebnis in Erfahrung zu bringen.

Typischer Arbeitsablauf

- Nutzen Sie Filter, um in der Backup-Plan-Tabelle die gewünschten Backup-Pläne (Tasks) zu sehen. Standardmäßig zeigt die Tabelle die Pläne der verwalteten Maschine nach Namen sortiert an. Sie können außerdem nicht benötigte Spalten ausblenden bzw. ausgeblendete wieder aktivieren. Zu weiteren Informationen siehe 'Tabellenelemente sortieren, filtern und konfigurieren (S. 29)'.
- Wählen Sie in der Tabelle den Backup-Plan (Task).
- Verwenden Sie die Schaltflächen der Symbolleiste, um eine Aktion auf den gewählten Plan (Task) anzuwenden. Zu Details siehe den Abschnitt Aktionen fьr zentrale Backup-Plдne und Tasks (S. 424).
- Verwenden Sie den Bereich 'Informationen' im unteren Teil des Fensters, um detaillierte Informationen über den gewählten Plan (Task) einsehen zu können. Die Leiste ist standardmäßig eingeklappt. Sie können den Fensterbereich aufklappen, indem Sie auf das Pfeilsymbol ▲

klicken. Der Inhalt der Leiste wird außerdem auch in den Fenstern **Plan-Details** (S. 370) und **Task-Details** (S. 372) angezeigt.

15.4.4.1 Aktionen für zentrale Backup-Pläne und Tasks

Nachfolgend finden Sie eine Anleitung zur Durchführung von Aktionen mit Tasks und zentralen Backup-Plänen.

Aufgabe	Lösung
Einen neuen Backup-Plan oder einen Task auf einer registrierten Maschine erstellen	Klicken Sie auf **Neu** und wählen Sie eine der folgenden Optionen: ▪ Backup-Plan (zentral) (S. 396) ▪ Recovery-Task (S. 146) ▪ Validierungstask (S. 266) Bei Erstellung eines Recovery- oder Validierungstasks müssen Sie die registrierte Maschine spezifizieren, auf der der gewählte Task laufen soll.
Details eines Plans/Tasks einsehen	Klicken Sie auf **Details anzeigen**. Überprüfen Sie dann im Fenster **Plan-Details/Task-Details** alle Informationen, die sich auf den gewählten Task beziehen.
Log eines Plans/Tasks einsehen	Klicken Sie auf **Log anzeigen**. Die Ansicht Log (S. 435) wird eine Liste der Log-Einträge anzeigen, die sich auf den gewählten Plan/Task beziehen.
Einen Backup-Plan/Task ausführen	**Backup-Plan** 1. Klicken Sie auf **Ausführen**. 2. Wählen Sie aus dem Listenfeld den Task des Plans aus, den Sie ausführen müssen. Die Ausführung eines Backup-Plans startet auch unmittelbar den dazugehörigen, ausgewählten Task, ungeachtet seiner Planung und der Bedingungen auf den Maschinen, wohin der Plan bereitgestellt wird. Ein zentraler Backup-Plan kann nicht manuell ausgeführt werden, falls auf mindestens einer der im Plan enthaltenen Maschinen ein Agent von Acronis Backup & Recovery 10 läuft. **Task** Der Tasks wird unmittelbar ausgeführt, ungeachtet seiner Planung.
Einen laufenden Backup-Plan/Task stoppen	Klicken Sie auf **Stopp**. **Zentraler Backup-Plan** Wenn Sie einen laufenden Backup-Plan stoppen, werden auch all seine Tasks auf allen Maschinen gestoppt, auf denen der Plan bereitgestellt wurde. Folglich werden alle Task-Aktionen abgebrochen. Ein zentraler Backup-Plan kann nicht manuell gestoppt werden, falls auf mindestens einer der im Plan enthaltenen Maschinen der Acronis Backup & Recovery 10 Agent läuft. **Task** Üblicherweise führt das Stoppen eines Tasks auch zum Abbruch seiner Aktionen (Backup, Wiederherstellung, Validierung, Export, Konvertierung, etc.). Der Task wechselt in das Stadium **Inaktiv**. Die Task-Planung bleibt aber, sofern erstellt,

Aufgabe	Lösung
	weiter gültig. Um die Aktion abzuschließen, müssen Sie den Task einmal erneut ausführen.
Einen Plan/Task editieren	Klicken Sie auf **Bearbeiten**. **Zentraler Backup-Plan** Die Bearbeitung eines zentralen Backup-Plans wird auf die gleiche Weise durchgeführt wie die Erstellung. Sobald ein Plan bearbeitet wird, aktualisiert der Management Server den Plan auf allen Maschinen, auf denen der Plan bereitgestellt wurde. **Task** Die Bearbeitung eines Tasks wird auf die gleiche Weise durchgeführt wie seine Erstellung.
Einen Backup-Plan klonen	Klicken Sie auf **Klonen**. Der Klon des ursprünglichen Backup-Plans wird mit dem Standardnamen '*Klon von <ursprünglicher Plan-Name>*' erstellt. Der geklonte Plan wird unmittelbar nach dem Klonvorgang deaktiviert, damit er nicht gleichzeitig mit dem ursprünglichen Plan ausgeführt wird. Sie können die Einstellungen des geklonten Plans bearbeiten, bevor Sie ihn dann aktivieren.
Einen Plan aktivieren	Klicken Sie auf **Aktivieren**. Der zuvor deaktivierte Backup-Plan wird wieder neu gemäß seiner Planung ausgeführt.
Einen Plan deaktivieren	Klicken Sie auf **Deaktivieren**. Der Backup-Plan wird nicht mehr gemäß seiner Planung ausgeführt. Er kann jedoch manuell gestartet werden. Der Plan verbleibt ansonsten auch nach einer manuellen Ausführung deaktiviert. Der Plan wird wieder wie normal ausgeführt, wenn Sie ihn erneut aktivieren.
Einen Plan exportieren	Klicken Sie auf **Exportieren**. Spezifizieren Sie Pfad und Namen für die resultierende Datei. Zu weiteren Informationen siehe 'Export und Import von Backup-Plдnen (S. 366)'.
Einen Plan importieren	Klicken Sie auf **Importieren**. Spezifizieren Sie den Pfad und Namen der Datei, die einen zuvor exportierten Plan enthält. Zu weiteren Informationen siehe 'Export und Import von Backup-Plдnen (S. 366)'.
Einen Plan/Task löschen	Klicken Sie auf **Löschen**. **Zentraler Backup-Plan** Daraufhin wird der zentrale Backup-Plan von den Maschinen, auf denen er bereitgestellt wurde, entfernt und vom Management Server gelöscht. Wenn die Maschine momentan offline ist, wird der Plan entfernt, sobald die Maschine wieder online ist. **Task** Als Folge wird der Task vom Management Server gelöscht. Die integrierten Verdichtungstasks und Storage Nodes können nicht gelöscht werden.

15.4.5 Storage Node

Der Acronis Backup & Recovery 11.5 Storage Node hilft Ihnen, die Verwendung verschiedener Ressourcen zu optimieren, die zum Schutz von Unternehmensdaten erforderlich sind. Dieses Ziel wird durch Organisation der verwalteten Depots erreicht, die als dedizierte Speicher für die Backup-Archive des Unternehmens dienen.

Die Storage Nodes stehen in der Ansicht **Storage Nodes** zur Verfügung, sobald Sie sie auf dem Management Server installiert und registriert haben. Zu weiteren Informationen über Aktionen mit Storage Nodes siehe den Abschnitt 'Storage Nodes (S. 247)'.

15.4.6 Lizenzen

Die Ansicht **Lizenzen** ermöglicht Ihnen, die auf dem Acronis License Server gespeicherten Lizenzen zu verwalten. Der License Server kann entweder in den Acronis Backup & Recovery 11.5 Management Server integriert sein oder als separate Komponente installiert werden.

Zugriff auf die Ansicht 'Lizenzen'

Um bei einer Verbindung mit dem Management Server auf die Ansicht **Lizenzen** zugreifen zu können, müssen Sie im Fensterbereich **Navigation** auf **Lizenzen** klicken.

So verbinden Sie sich direkt mit dem License Server:

1. Wählen Sie in der Konsole im Menü **Werkzeuge** den Befehl **Lizenzen verwalten**.
2. Geben Sie den Namen oder die IP-Adresse der Maschine des License Servers an.
3. Klicken Sie auf **OK**. Darauf öffnet sich die gleiche Ansicht **Lizenzen**.

Informationen zu Lizenzen anzeigen

In der Ansicht **Lizenzen** werden alle Lizenzschlüssel angezeigt, die auf dem License Server vorhanden sind. Die Schlüssel sind nach Produkten gruppiert. Eine Lizenz kann mehrere Einzellizenzen enthalten.

Klicken Sie mit der rechten Maustaste auf die Spaltenüberschriften, um auszuwählen, welche Details angezeigt werden: Lizenzschlüssel, Ablaufdatum, Importdatum und Gesamtzahl der Lizenzschlüssel sowie Informationen darüber, wie viele der Lizenzen verfügbar (d.h. frei) sind oder verwendet werden.

Erweitern Sie das benötigte Produkt und dann den entsprechenden Schlüssel, um mehr Informationen über jeden einzelnen Lizenzschlüssel einsehen zu können. Klicken Sie auf **Maschinen anzeigen, die die Lizenz verwenden**, um weitere Informationen über die Maschinen zu erhalten, die eine Lizenz nutzen.

15.4.6.1 Lizenzen hinzufügen

Fügen Sie Lizenzen zuerst dem License Server hinzu, um sie verwalten zu können.

So fügen Sie Lizenzen hinzu

1. Klicken Sie auf **Lizenz hinzufügen**.
2. Geben Sie im Fenster **Hinzuzufügende Lizenzen spezifizieren** die Lizenzschlüssel ein oder importieren Sie diese aus einer Datei. Um Lizenzen von einer .txt-, .eml- oder .xml-Datei importieren zu können, klicken Sie auf **Schlüssel aus Datei importieren** und spezifizieren Sie dann die Datei, die die Liste der Lizenzschlüssel enthält. Sie können mehrere Dateien nacheinander spezifizieren oder die Lizenzschlüssel auch manuell eingeben.
3. Klicken Sie auf **OK**.

15.4.6.2 Den vom Management Server verwendeten License Server ändern

Der Management Server verwendet standardmäßig den integrierten License Server. Sie können den Management Server dazu bringen, einen anderen License Server zu verwenden. Falls Sie bereits einen separaten License Server haben, kann Ihnen diese Funktionalität helfen, den License Server auf neue Hardware zu migrieren.

Stellen Sie vor dem Wechsel des License Servers sicher, dass Sie die Lizenzen von dem alten License Server exportieren (S. 427) und diese danach dem neuen hinzufьgen (S. 426).

So wechseln Sie den License Server

1. Verbinden Sie die Konsole mit dem Management Server.
2. Wählen Sie im Menü **Aktionen** den Befehl **License Server wechseln**.
3. Geben Sie den Namen oder die IP-Adresse der Maschine des License Servers an.
4. Klicken Sie auf **OK**.

Der Management Server stellt nach dem Wechsel des License Servers die IP-Adresse des neuen License Servers den registrierten Maschinen bereit, so dass diese den neuen License Server verwenden können.

15.4.6.3 Lizenzen exportieren

Bevor Sie einen License Server wechseln, sollten Sie die Lizenzen von dem License Server exportieren, den Sie wechseln (S. 427) wollen. Alle Lizenzen werden in einer .xml-Datei gespeichert. Sie können diese Lizenzen dann später in den neuen License Server importieren (S. 426).

So exportieren Sie Lizenzen

1. Klicken Sie auf **Lizenzen nach XML exportieren**.
2. Spezifizieren Sie den Zielort für die Datei (und optional den Dateinamen).
3. Klicken Sie auf **OK**, um die Datei zu speichern.

15.4.6.4 Lizenzen entfernen

Um eine Lizenz vollständig vom Acronis License Server zu entfernen, wählen Sie diese aus der Liste der verfügbaren Lizenzen und klicken Sie in der Symbolleiste auf **Lizenz entfernen**. Um eine in Benutzung befindliche Lizenz zu entfernen, müssen Sie diese zuerst widerrufen (S. 427).

15.4.6.5 Lizenzen widerrufen

Durch Widerrufen werden verwendete Lizenzen erneut verfügbar gemacht. Das kann für Sie in folgenden Fällen erforderlich sein:

- Eine Komponente, die eine Lizenz benötigt (etwa ein Agent), wird von einer Maschine deinstalliert.

  Widerrufen Sie die Lizenz von der Maschine entweder bevor oder nachdem Sie die Komponente deinstallieren.
- Eine verwaltete Maschine wird dauerhaft außer Betrieb genommen.

  Widerrufen Sie die Lizenz von der Maschine entweder bevor oder nachdem Sie die Maschine ausrangieren.

Stellen Sie sicher, dass die Widerrufung und nachfolgende Verwendung einer Lizenz nicht gegen die Lizenzvereinbarung oder andere rechtliche Bestimmungen verstößt.

So widerrufen Sie eine Lizenz:

Erweitern Sie das benötigte Produkt und dann den entsprechenden Lizenzschlüssel.

- Falls der Lizenzschlüssel von einer einzelnen Maschine verwendet wird, klicken Sie in der Symbolleiste auf **Lizenz widerrufen**.
- Falls der Lizenzschlüssel von mehreren Maschinen genutzt wird, klicken Sie auf **Maschinen anzeigen, die die Lizenz verwenden**. Wählen Sie im erscheinenden Fenster den Host, von dem Sie die Lizenz widerrufen möchten (siehe die Spalte **Host-Name**) und klicken Sie auf **Lizenz widerrufen**.

15.4.6.6 Verwenden des Verwaltungswerkzeugs des Acronis License Server

Die Datei 'LicenseServerCmdLine.exe' befindet sich im Installationsordner des License Servers, der standardmäßig dem Ordner '\Programme\Acronis\LicenseServer' entspricht.

LicenseServerCmdLine.exe verwendet folgende Syntax:

```
LicenseServerCmdLine <Befehl> <Parameter1> <Parameter2>
```

LicenseServerCmdLine.exe unterstützt folgende Parameter:

```
--status <IP-Adresse oder Host-Name>
```

Zeigt die Gesamtzahl an Lizenzen sowie die Anzahl der für jedes Acronis-Produkt verfügbaren Lizenzen an.

```
--import <IP-Adresse oder Host-Name> <Lizenzschlüssel>
```

Fügt dem angegebenen License Server eine neue Lizenz hinzu. Sie können mehrere Lizenzen angeben (durch Leerzeichen voneinander getrennt).

```
--import-file <IP-Adresse oder Host-Name> <Dateiname>
```

Importiert Lizenzen aus einer TXT- oder EML-Datei.

```
--help
```

Zeigt die Verwendung.

15.4.7 Alarmmeldungen

Ein Alarm ist eine Nachricht, die vor gegenwärtigen oder potentiellen Problemen warnt. In der Ansicht **Alarmmeldungen** können Sie die Probleme schnell identifizieren und lösen, indem Sie die aktuellen Alarmmeldungen überwachen und den Alarmverlauf einsehen.

Aktive und inaktive Alarmmeldungen

Ein Alarm kann sich entweder in einem aktiven oder inaktiven Stadium befinden. Ein aktives Stadium bedeutet, dass das Problem, welches den Alarm verursacht hat, immer noch existiert. Ein aktiver Alarm wird inaktiv, wenn das Problem, das den Alarm verursacht hat, entweder manuell oder von alleine gelöst wurde.

***Anmerkung**: Es gibt einen Alarmtyp, der immer aktiv ist: „Backup nicht erstellt“. Hintergrund ist, dass selbst bei erfolgreicher Behebung der Alarmursache und erfolgreicher Erstellung anderer, nachfolgender Backups, die Tatsache immer noch bestehen bleibt, dass das Backup nicht erstellt wurde.*

Probleme beheben, die Alarmmeldungen verursacht haben

Klicken Sie auf **Problem beheben**, um die Alarmursache herauszufinden und zu beseitigen. Sie werden daraufhin zur entsprechenden Ansicht geführt,wo Sie das Problem untersuchen und die notwendigen Schritte zu seiner Lösung durchführen können.

Sie können optional auch auf **Details anzeigen** klicken, um mehr Informationen über den von Ihnen gewählten Alarm zu erhalten.

Alarmmeldungen annehmen

Standardmäßig listet die Tabelle **Aktuelle Alarmmeldungen** sowohl aktive als auch inaktive Alarmmeldungen auf, solange bis diese nicht mehr akzeptiert werden. Um einen Alarm anzunehmen, wählen Sie diesen aus und klicken dann auf den Befehl **Annehmen**. Indem Sie einen Alarm annehmen, nehmen Sie ihn zur Kenntnis und übernehmen dieVerantwortung für ihn. Die angenommenen Alarmmeldungen werden dann ohne Änderung ihres Alarmstadiums zur Tabelle **Angenommene Alarmmeldungen** verschoben.

Die Tabelle **Angenommene Alarmmeldungen** speichert so einen Verlauf aller angenommenen Alarmmeldungen. Sie können hier herausfinden, wer einen Alarm angenommen hat und wann sich dieser ereignete. Angenommene Alarmmeldungen beider Stadien können aus der Tabelle entweder manuell entfernt werden – durch Verwendung der Schaltflächen **Löschen** und **Alle löschen** – oder automatisch entfernt werden (siehe „Alarmmeldungen konfigurieren“ weiter unten in diesem Abschnitt).

Indem Sie auf **Alle in Datei speichern** klicken, können Sie den kompletten Tabelleninhalt in eine *.txt- oder *.csv-Datei exportieren.

Anzeige der Alarmmeldungen auf dem Management Server

Wenn die Konsole mit dem Management Server verbunden ist, werden in der Ansicht **Alarmmeldungen** sowohl die Alarmmeldungen angezeigt, die von den registrierten Maschinen gesammelt wurden, wie auch die des Management Servers.

Von registrierten Maschinen gesammelte Alarmmeldungen:

- Erscheinen in der Anzeige **Alarmmeldungen** unabhängig von diesen Maschinen
- Werden separat angenommen, sowohl auf Seite des Management Servers wie auf den registrierten Maschinen.

Ähnliche, von mehreren Maschinen gesammelte Alarmmeldungen werden zu einem einzigen Gruppenalarm kombiniert. Bei Gruppenalarmmeldungen sieht die Spalte **Maschine** aus wie **Mehrfach (X)**, wobei **X** der Anzahl an registrierten Maschinen mit diesem Alarm entspricht. Sobald ein einzelner aktiver Alarm in der Gruppe inaktiv wird, wird der Alarm zu einer neuen oder einer bereits existierenden inaktiven Gruppe verschoben. Die Zahl der assoziierten Maschinen (**X**) für den aktiven Gruppenalarm nimmt entsprechend ab, während die für den inaktiven Gruppenalarm zunimmt.

Klicken Sie auf **Details anzeigen**, um Informationen über die Maschinen zu erhalten, die mit dem Gruppenalarm assoziiert sind.

Alarmmeldungen konfigurieren

Verwenden Sie zur Konfiguration von Alarmmeldungen folgende Optionen aus dem oberen Bereich der Anzeige **Alarmmeldungen**.

- **Alarmmeldungen anzeigen/verbergen** (S. 31) – spezifizieren Sie den Alarmtyp, der in der Ansicht **Alarmmeldungen** angezeigt werden soll.
- **Benachrichtigungen** (S. 441) – konfigurieren Sie die E-Mail-Benachrichtigungen über Alarmmeldungen.
- **Einstellungen** (S. 438) – spezifizieren Sie, ob inaktive Alarmmeldungen automatisch in die Tabelle **Angenommene Alarmmeldungen** verschoben werden sollen; konfigurieren Sie, wie lange die angenommenen Alarmmeldungen in der Tabelle **Angenommene Alarmmeldungen** bewahrt werden sollen.

15.4.8 Berichte

Mit der Berichtsfunktion stehen dem Administrator des Management Server detaillierte und wohlstrukturierte Informationen über die Sicherung von Unternehmensdaten zur Verfügung. Die Berichte dienen als Werkzeug für eine gründliche Analyse der gesamten Backup-Infrastruktur innerhalb des Unternehmensnetzwerks.

Der Management Server erstellt Berichte anhand von Statistiken und Logs, die auf den registrierten Maschinen gesammelt und in den dedizierten Datenbanken gespeichert werden.

Berichtsvorlagen

Die Berichte werden basierend auf Berichtsvorlagen erstellt. In den Vorlagen ist definiert, welche Informationen ein Bericht enthalten soll und wie diese Informationen dargestellt werden sollen.

Acronis Backup & Recovery 11.5 Management Server bietet Berichtsvorlagen für:

- Registrierte Maschinen.
- Auf den registrierten Maschinen vorliegende lokale und zentrale Backup-Pläne.
- Auf den registrierten Maschinen vorliegende lokale und zentrale Tasks.
- In den zentral verwalteten Depots gespeicherte Archive und Backups.
- Statistiken über zentral verwaltete Depots.
- Verlaufshistorie der Task-Aktivitäten.

Berichte über Maschinen, Backup-Pläne, Tasks, Archive und Backups enthalten Informationen ab dem gegenwärtigen Zeitpunkt.

Berichte über Depot-Statistiken und Task-Aktivitäten sind intervallbasiert und bieten zurückliegende Informationen für ein angegebenes Zeitintervall, welches von Tagen bis Jahren reichen kann (abhängig von der in den Datenbanken enthaltenen Datenmenge).

Berichte konfigurieren und generieren

Es gibt zwei Typen von Berichtsvorlagen: benutzerdefinierbar und vordefiniert.

In einer benutzerdefinierbaren Berichtsvorlage können Sie mit Filtern spezifizieren, welche Einträge in den Bericht aufgenommen werden sollen und wie diese gruppiert und sortiert werden sollen. Um einen Bericht zu konfigurieren, wählen Sie eine Berichtsvorlage aus der Ansicht **Berichte**, dann klicken Sie in der Symbolleiste auf **Konfigurieren** und anschließend stellen Sie die **Filter** sowie die **Berichtsanzeige** ein. Klicken Sie auf **OK**, damit der Bericht generiert wird.

Eine vordefinierte Berichtsvorlage ist vorgegeben, so dass Sie einen Report mit einem Klick generieren können. Um einen Bericht zu erstellen, wählen Sie eine Berichtsvorlage in der Ansicht **Berichte** und klicken dann in der Symbolleiste auf **Generieren**.

Die Informationen des Berichts werden entsprechend der Vorlageneinstellungen selektiert, gruppiert und sortiert. Wählen Sie, ob Sie eine Vorschau des Berichts in Ihrem Standard-Browser sehen wollen oder ob er direkt in eine .xml-Datei gespeichert werden soll. Bei der Vorschau erscheint der Bericht in einem separaten, interaktiven Fenster, in dem Sie die Tabellen erweitert oder reduziert können. Verwenden Sie Microsoft Excel oder Microsoft Access, um die gespeicherte .xml-Datei zu öffnen.

15.4.8.1 Bericht über Maschinen

In dieser Ansicht können Sie Berichte über die Maschinen erstellen, die auf dem Management Server registriert sind. Ein solcher Bericht besteht aus einer oder mehreren Tabelle(n).

Filter

Unter **Filter** bestimmen Sie, welche Maschinen in den Bericht aufgenommen werden sollen. Nur die Maschinen, die alle Filterkriterien erfüllen, werden aufgenommen.

- **Maschinen**: Liste der Maschinen. Wählen Sie entweder Maschinen mit Agenten oder virtuelle Maschinen. [Optional] Klicken Sie auf **Auswahl**, um bestimmte Maschinen oder Maschinengruppen wählen zu können.
- **Status**: Der Status der Maschinen – **OK**, **Warnung** bzw. **Fehler**.
- **Letzte Verbindung** (nur Maschinen mit Agenten): Der Zeitraum, innerhalb dessen die letzte Verbindung zwischen den Maschinen und dem Management Server erfolgte.
- **Letztes erfolgreiches Backup**: Der Zeitraum, innerhalb dessen das letzte erfolgreiche Backup auf jeder der Maschinen beendet wurde.
- **Nächstes Backup**: Der Zeitraum, innerhalb dessen das nächste geplante Backup auf jeder der Maschinen starten wird.
- **Betriebssystem**: Die Betriebssysteme, die auf den Maschinen laufen.
- **IP-Adresse** (nur Maschinen mit Agenten): Der Adressbereich der letzten bekannten IP-Adressen für die Maschinen.
- **Verfügbarkeit** (nur Maschinen mit Agenten): Die Verfügbarkeit der Maschinen – **Online** oder **Offline**.

Mit den Standardfiltereinstellungen enthält der Bericht alle Maschinen mit Agenten.

Berichtsansicht

In der **Berichtsansicht** bestimmen Sie das Aussehen des Berichts:

- Legen Sie fest, ob alle Elemente in einer Tabelle angezeigt oder nach einer bestimmten Spalte sortiert werden sollen.
- Geben Sie an, welche Tabellenspalten in welcher Reihenfolge angezeigt werden sollen.
- Geben Sie an, wie die Tabelle sortiert werden soll.

15.4.8.2 Bericht über Backup-Pläne

In dieser Ansicht können Sie Berichte über die Backup-Pläne auf den registrierten Maschinen erstellen. Ein solcher Bericht besteht aus einer oder mehreren Tabelle(n).

Filter

Unter **Filter** bestimmen Sie, welche Backup-Pläne in den Bericht aufgenommen werden sollen. Nur die Backup-Pläne, die alle Filterkriterien erfüllen, werden aufgenommen.

- **Ursprung**: Die Planungsart der Backup-Pläne – **Lokal** oder **Zentral**.

- **Maschinen**: Die Liste der Maschinen, auf denen sich die Backup-Pläne befinden.
- **Gesicherter Datentyp**: Die Typen der im Backup vorliegenden Daten – **Maschinen/Laufwerke/Volumes** und/oder **Dateien**.
- **Deployment-Stadium**: Die Deployment-Stadien der Backup-Pläne – beispielsweise **Wird widerrufen**.
- **Ausführungsstadium**: Das Ausführungsstadium der Backup-Pläne – z.B. **Laufend**.
- **Status**: Die Zustände der Backup-Pläne – **OK**, **Warnung** bzw. **Fehler**.
- **Letzte Abschlusszeit**: Der Zeitpunkt, zu dem der letzte Task des Backup-Plans abgeschlossen wurde.
- **Planung**: Die Planungsart der Backup-Pläne – **Manuell** oder **Geplant**. Bei der manuellen Planung muss die Ausführung eines Backup-Plans manuell gestartet werden.
- **Besitzer**: Die Liste der Benutzer, die die Backup-Pläne erstellt haben.

In der Standardeinstellung werden alle Backup-Pläne auf allen Maschinen in den Bericht aufgenommen.

Berichtsansicht

In der **Berichtsansicht** bestimmen Sie das Aussehen des Berichts:

- Legen Sie fest, ob alle Elemente in einer Tabelle angezeigt oder nach einer bestimmten Spalte sortiert werden sollen.
- Geben Sie an, welche Tabellenspalten in welcher Reihenfolge angezeigt werden sollen.
- Geben Sie an, wie die Tabelle sortiert werden soll.

15.4.8.3 Bericht über Tasks

In dieser Ansicht können Sie Berichte über die Tasks erstellen, die auf den registrierten Maschinen ausgeführt werden. Ein solcher Bericht besteht aus einer oder mehreren Tabelle(n).

Filter

Unter **Filter** bestimmen Sie, welche Tasks in den Bericht aufgenommen werden sollen. Nur die Tasks, die alle Filterkriterien erfüllen, werden aufgenommen.

- **Ursprung**: Der Ursprung der Tasks – **Zentral**, **Lokal** bzw. **Lokal ohne Backup-Plan**. Zentrale Tasks gehören zu einem zentralen Backup-Plan. Lokale Tasks (z.B. ein Recovery-Task) gehören nicht unbedingt zu einem Backup-Plan.
- **Backup-Pläne** (nur zentrale Tasks): Die Backup-Pläne, auf denen die Tasks basieren.
- **Maschinen**: Die Liste der Maschinen, auf denen sich die Tasks befinden.
- **Typ**: Die Task-Typen – z.B. Tasks für Disk-Backups.
- **Ausführungsstadium**: Die Ausführungsstadien der Tasks – z.B. **Läuft**.
- **Letztes Ergebnis**: Die letzten Ergebnisse der Tasks – **Erfolgreich abgeschlossen**, **Mit Warnungen abgeschlossen**, **Fehlgeschlagen**, **Gestoppt** oder '**–**' (bisher ohne Ergebnis).
- **Planung**: Die Planungsart der Tasks – **Manuell** oder **Geplant**. Bei der manuellen Planung muss die Ausführung eines Tasks manuell gestartet werden.
- **Besitzer**: Die Liste der Benutzer, die die Tasks erstellt haben.
- **Dauer**: Anfang und Ende des Zeitraums, in dem die einzelnen Tasks zuletzt ausgeführt wurden.

In der Standardeinstellung werden alle Tasks auf allen Maschinen in den Bericht aufgenommen.

Berichtsansicht

In der **Berichtsansicht** bestimmen Sie das Aussehen des Berichts:

- Legen Sie fest, ob alle Elemente in einer Tabelle angezeigt oder nach einer bestimmten Spalte sortiert werden sollen.
- Geben Sie an, welche Tabellenspalten in welcher Reihenfolge angezeigt werden sollen.
- Geben Sie an, wie die Tabelle sortiert werden soll.

15.4.8.4 Bericht über Archive und Backups

In dieser Ansicht können Sie Berichte über die Archive erstellen, die in zentral verwalteten Depots gespeichert sind. Ein solcher Bericht besteht aus einer oder mehreren Tabelle(n).

Filter

Unter **Filter** bestimmen Sie, welche Archive in den Bericht aufgenommen werden sollen. Nur die Archive, die alle Filterkriterien erfüllen, werden aufgenommen.

- **Depots**: Die Liste der zentral verwalteten Depots, in denen die Archive gespeichert sind.
- **Maschinen**: Die Liste der registrierten Maschinen, auf denen die Archive erstellt worden sind.
- **Typ**: Die Archiv-Typen – laufwerksbasierte bzw. dateibasierte Archive.
- **Besitzer**: Die Liste der Benutzer, die die Archive erstellt haben.
- **Erstellungszeit**: Der Zeitraum seit Erstellen des letzten Backup in den einzelnen Archiven.
- **Belegter Speicherplatz**: Der Speicherplatz, den die einzelnen Archive belegen.
- **Gesicherte Daten**: Die Begrenzungen für die Gesamtgröße aller Daten, die gegenwärtig in den einzelnen Archiven gespeichert sind. Diese Größe kann sich durch Komprimierung oder Deduplizierung von der des belegten Speicherplatzes unterscheiden.
- **Zahl der Backups**: Die Beschränkungen für die Anzahl der Backups in den einzelnen Archive.

In der Standardeinstellung werden alle Archive, die in den zentral verwalteten Depots gespeichert sind, in den Bericht aufgenommen.

Berichtsansicht

In der **Berichtsansicht** bestimmen Sie das Aussehen des Berichts:

- Legen Sie fest, ob alle Elemente in einer Tabelle angezeigt oder nach einer bestimmten Spalte sortiert werden sollen.
- Geben Sie an, welche Tabellenspalten in welcher Reihenfolge angezeigt werden sollen.
- Geben Sie an, wie die Tabelle sortiert werden soll.

15.4.8.5 Bericht über Statistiken für Depots

In dieser Ansicht können Sie einen Bericht über die Nutzung der zentral verwalteten Depots erstellen, die gegenwärtig zum Management Server hinzugefügt werden. Ein solcher Bericht besteht aus einer oder mehreren Tabelle(n) und einem oder mehreren Diagramm(en).

Berichtsumfang

Unter **Berichtsumfang** bestimmen Sie den Zeitraum, für den der Bericht erstellt werden soll. Der Bericht wird das Stadium der gewählten Depots für die angegebene Zeit an jedem Tag des Berichtszeitraums darstellen.

Filter

Unter **Filter** bestimmen Sie, welche zentral verwalteten Depots in den Bericht aufgenommen werden sollen, und ob er eine Gesamtübersicht über alle ausgewählten Depots enthalten soll.

Diese Gesamtübersicht zeigt den gesamten freien und belegten Speicherplatz, die Gesamtmenge der gesicherten Daten, die Gesamtzahl der Archive und Backups, sowie die Durchschnittswerte für die ausgewählten Depots.

Mit den standardmäßigen Filtereinstellungen werden Informationen über alle zentral verwalteten Depots sowie die Gesamtsumme in den Bericht aufgenommen.

Berichtsansicht

In der **Berichtsansicht** bestimmen Sie das Aussehen des Berichts:

- Geben Sie an, welche Tabellenspalten in welcher Reihenfolge angezeigt werden sollen.
- Geben Sie an, welche Diagramme in den Bericht aufgenommen werden sollen. Die Diagramme zeigen die Speicherplatzbelegung in den Depots an.

15.4.8.6 Bericht über Task-Aktivitäten

In dieser Ansicht können Sie Berichte über die Tasks erstellen, die sich in einem von Ihnen gewählten Zeitraum auf den registrierten Maschinen befanden. Solch ein Bericht besteht aus einem oder mehreren Diagramm(en) – ein Diagramm pro Maschine.

Die Diagramme zeigen an, wie oft an einem bestimmten Tag die einzelnen Tasks mit einem dieser Ergebnisse beendet wurden: „Erfolgreich abgeschlossen“, „Mit Warnungen abgeschlossen“ und „Fehlgeschlagen“.

Berichtsumfang

Unter **Berichtsumfang** bestimmen Sie den Zeitraum, für den der Bericht erstellt werden soll.

Filter

Unter **Filter** bestimmen Sie, welche Tasks in den Bericht aufgenommen werden sollen. Nur die Tasks, die alle Filterkriterien erfüllen, werden aufgenommen.

- **Ursprung**: Der Ursprung der Tasks – **Zentral**, **Lokal** bzw. **Lokal ohne Backup-Plan**. Zentrale Tasks gehören zu einem zentralen Backup-Plan. Lokale Tasks (z.B. ein Recovery-Task) gehören nicht unbedingt zu einem Backup-Plan.
- **Backup-Pläne** (nur zentrale Tasks): Die Backup-Pläne, auf denen die Tasks basieren. Die Standardeinstellung entspricht allen Backup-Plänen aus dem entsprechenden Berichtszeitraum.
- **Maschinen**: Die Liste der Maschinen, auf denen sich die Tasks befinden.
- **Typ**: Die Task-Typen – z.B. Tasks für Disk-Backups.
- **Besitzer**: Die Liste der Benutzer, die die Tasks erstellt haben.

In der Standardeinstellung werden alle Tasks, die sich zu irgendeiner Zeit während des Berichtszeitraum auf den registrierten Maschinen befanden, in den Bericht aufgenommen.

15.4.8.7 Spaltenauswahl

Im Fenster **Spaltenauswahl** bestimmen Sie, welche Tabellenspalten in welcher Reihenfolge in den Bericht aufgenommen werden sollen.

Die Tabellenspalten werden im Bericht entsprechend der Liste **Im Bericht anzeigen** dargestellt. Dabei entspricht der oberste Listeneintrag der Spalte ganz links im Bericht.

Verwenden Sie bei der Auswahl der anzuzeigenden Spalten die Pfeiltasten links und rechts um Spalten aus – oder abzuwählen, und die Pfeiltasten oben und unten um die Reihenfolge der Spalten zu ändern.

Einige Spalten – z.B. **Maschinenname** in einem Bericht über Maschinen – können nicht abgewählt oder nach oben bzw. unten verschoben werden.

15.4.8.8 Berichtsansicht

Ermögliche Sie die Ausführung 'Aktiver Inhalte' (JavaScript) in Ihrem Webbrowser, damit Datums- und andere Informationen in den erstellten Berichten korrekt angezeigt werden. Sie können die Ausführung 'Aktiver Inhalte' für die aktuelle Webseite temporär zulassen oder sie auch permanent aktivieren. Um die Ausführung 'Aktiver Inhalte' im Internet Explorer temporär einzuschalten, klicken Sie auf die standardmäßig am Kopf der Webseite erscheinende Informationsleiste und dann auf **Blockierte Inhalte zulassen**.

Um 'Aktive Inhalte' dauerhaft zuzulassen

klicken Sie im Internet Explorer

1. im Menü **Extras** auf **Internetoptionen** und dann auf die Registerlasche **Erweitert**.
2. Aktivieren Sie im Abschnitt **Sicherheit** das Kontrollkästchen **Ausführung aktiver Inhalte in Dateien auf dem lokalen Computer zulassen**.
3. Klicken Sie auf **OK**.

in Mozilla Firefox

1. Klicken Sie im Menü **Extras, Einstellungen** auf **Inhalt**.
2. Stellen Sie sicher, dass das Kontrollkästchen **JavaScript aktivieren** angewählt ist.
3. Klicken Sie auf **OK**.

15.4.9 Log

Das zentrale Ereignis-Log speichert den Verlauf der Aktivitäten, die vom Management Server, den Storage Nodes und den registrierten Maschinen ausgeführt wurden.

Wählen Sie zur Anzeige einer einfachen Liste von Log-Einträgen das Element **Ereignisse** aus dem Listenfeld **Anzeige** – um nach Aktivitäten gruppierte Log-Einträge angezeigt zu bekommen, wählen Sie **Aktivitäten**. Details zu einem ausgewählten Log-Eintrag oder einer Aktivität werden im Fensterbereich **Informationen** angezeigt (im unteren Teil der **Log**-Anzeige).

Verwenden Sie Filter, um gewünschte Aktivitäten und Log-Einträge in der Tabelle anzeigen zu lassen. Sie können außerdem nicht benötigte Spalten ausblenden bzw. ausgeblendete wieder aktivieren. Zu Details siehe Tabellenelemente sortieren, filtern und konfigurieren (S. 29). Wenn Sie Elemente in anderen administrativen Ansichten ausgewählt haben (**Dashboard**, **Maschinen mit Agenten**, **Backup-Pläne und Tasks**), dann können Sie die **Log**-Ansicht mit bereits vorgefilterten Log-Einträgen für das betreffende Element öffnen.

Wählen Sie eine Aktivität oder Log-Eintrag aus, um auf diese eine Aktion ausführen zu lassen. Zu Details siehe 'Aktionen fьr Log-Eintrдge (S. 436)' und 'Details zu Log-Eintrдgen (S. 437)'.

15.4.9.1 Aktionen für Log-Einträge (zentral)

Alle nachfolgend beschriebenen Aktionen werden durch Klicken auf die korrespondierenden Elemente in der Log-**Symbolleiste** ausgeführt. Diese Aktionen können außerdem über das Kontextmenü durchgeführt werden (indem Sie mit der rechten Maustaste auf den Log-Eintrag oder die Aktivität klicken).

Nachfolgend finden Sie eine Anleitung zur Ausführung von Aktionen auf Log-Einträge.

Aufgabe	Lösung
Eine einzelne Aktivität wählen	Wählen Sie **Aktivitäten** aus dem Listenfeld **Anzeige** und klicken Sie dann auf die gewünschte Aktivität. Im Fensterbereich **Informationen** werden für die gewählte Aktivität die Log-Einträge angezeigt.
Einen einzelnen Log-Eintrag wählen	Klicken Sie auf ihn.
Mehrere Log-Einträge wählen	▪ *Nicht zusammenhängend*: Halten Sie **Strg** gedrückt und klicken Sie nacheinander auf die gewünschten Log-Einträge ▪ *Zusammenhängend*: wählen Sie einen einzelnen Log-Eintrag, halten Sie dann die **Umschalt**-Taste gedrückt und klicken Sie auf einen weiteren Log-Eintrag. Darauf werden auch alle Log-Einträge zwischen der ersten und letzten Markierung ausgewählt.
Details zu einem Log-Eintrag einsehen	1. Wählen Sie einen Log-Eintrag. 2. Wählen Sie eine der nachfolgenden Varianten: ▪ Klicken Sie doppelt auf die Auswahl. ▪ Klicken Sie auf **Details**. Die Details des Log-Eintrags werden angezeigt. Zu Details über Aktionen für Log-Einträge siehe den Abschnitt 'Details zu Log-Eintrдgen (S. 437)'.
Gewählte Log-Einträge in eine Datei speichern	1. Lassen Sie die **Aktivitäten** anzeigen und wählen Sie die entsprechenden Aktivitäten oder lassen Sie die **Ereignisse** anzeigen und wählen Sie die entsprechenden Log-Einträge. 2. Klicken Sie auf **Auswahl in Datei speichern**. 3. Vergeben Sie im geöffneten Fenster einen Pfad und Namen für die Datei. Alle Log-Einträge der gewählten Aktivitäten oder gewählten Log-Einträge werden in eine spezifizierte Datei gespeichert.
Alle Log-Einträge in eine Datei speichern	1. Stellen Sie sicher, dass keine Filter gesetzt sind. 2. Klicken Sie auf **Alle in Datei speichern**. 3. Vergeben Sie im geöffneten Fenster einen Pfad und Namen für die Datei. Alle Log-Einträge werden in die spezifizierte Datei gespeichert.
Alle gefilterten Log-Einträge in eine Datei speichern	1. Setzen Sie Filter, um eine Liste von Log-Einträgen zu erhalten, die den Filterkriterien entsprechen. 2. Klicken Sie auf **Alle in Datei speichern**. 3. Vergeben Sie im geöffneten Fenster einen Pfad und Namen für die Datei. Alle Log-Einträge in der Liste werden in die spezifizierte Datei gespeichert.

Alle Log-Einträge löschen	Klicken Sie auf **Alle Löschen**. Alle Einträge werden aus dem Log gelöscht und es wird ein neuer Log-Eintrag erstellt. Er enthält Informationen darüber, wer die Log-Einträge gelöscht hat und wann.
Log-Level einrichten	Klicken Sie auf **Log-Level einstellen**. Spezifizieren Sie im Fenster **Log-Level** (S. 442) Ereignistypen, die von den registrierten Maschinen für das zentrale Log gesammelt werden sollen.

15.4.9.2 Details zum zentralen Log-Eintrag

Zeigt für den gewählten Log-Eintrag detaillierte Informationen an und erlaubt Ihnen, die Details in die Zwischenablage zu kopieren.

Um Details des nächsten oder vorherigen Log-Eintrages einsehen zu können, müssen Sie auf die Schaltfläche mit dem Pfeil nach unten bzw. oben klicken.

Klicken Sie auf die Schaltfläche **In Zwischenablage kopieren**, um die Details zu kopieren.

Datenfelder der Log-Einträge

Ein zentraler Log-Eintrag enthält die folgenden Datenfelder:

- **Typ** – Ereignistyp (Fehler, Warnung, Information).
- **Datum und Zeit** – Datum und Uhrzeit, wann das Ereignis stattfand.
- **Backup-Plan** – der Backup-Plan, auf den sich das Ereignis bezieht (sofern vorhanden).
- **Task** – Der Task, auf den sich das Ereignis bezieht (sofern vorhanden).
- **Typ der verwalteten Einheit** – Der Typ der verwalteten Einheit, in welcher das Ereignis aufgetreten ist (falls überhaupt).
- **Verwaltete Einheit** – Der Name der verwalteten Einheit, in welcher das Ereignis aufgetreten ist (falls überhaupt).
- **Maschine** – Der Name der Maschine, wo das Ereignis aufgetreten ist (sofern vorhanden).
- **Code** – Kann leer sein oder dem Programmfehlercode entsprechen, wenn das Ereignis vom Typ „Fehler“ ist. Der Fehlercode ist eine Integer-Zahl, die vom Acronis-Support zum Lösen des Problems verwendet werden kann.
- **Modul** – Kann leer sein oder der Nummer des Programmmoduls entsprechen, in dem ein Fehler aufgetreten ist. Es handelt sich um eine Integer-Zahl, die vom Acronis Support Service verwendet werden kann, um das Problem zu lösen.
- **Besitzer** – Der Benutzername des Backup-Plan-Besitzers (S. 35).
- **Nachricht** – Eine Textbeschreibung des Ereignisses.

15.4.10 Optionen des Management Servers

Die Optionen für den Management Server ermöglichen Ihnen, das Verhalten von Acronis Backup & Recovery 11.5 Management Server zu steuern.

Um auf die Optionen des Management Servers zuzugreifen, verbinden Sie die Konsole zum Management Server und wählen dann **Optionen > Management Server Optionen** im Menü.

15.4.10.1 Acronis WOL Proxy

Diese Option funktioniert in Kombination mit den erweiterten Planungseinstellungen für **Wake-on-LAN verwenden** (S. 98). Verwenden Sie diese Option, wenn der Management Server Maschinen zum Backup in einem anderen Subnetz einschalten soll.

Kurz bevor die geplante Aktion startet, verschickt der Management Server so genannte 'Magic Packets', um die entsprechenden Maschinen einzuschalten. (Ein 'Magic Packet' ist ein Paket, das 16 Mal in Folge die MAC-Adresse der Empfänger-Netzwerkkarte enthält). Der in dem anderen Subnetz installierte Acronis WOL Proxy sendet die Pakete an die Maschinen in diesem Subnetz.

Voreinstellung ist: **Deaktiviert**.

So aktivieren Sie diese Option:

1. Installieren Sie Acronis WOL Proxy auf einem Server im Subnetz, auf dem die Maschinen sich befinden, die Sie einschalten möchten. Bei diesem Server muss eine ständige Verfügbarkeit der Dienste gewährleistet sein. Wenn mehrere Subnetze vorhanden sind, installieren Sie Acronis WOL Proxy in jedem Subnetz, in dem Sie die Funktion Wake-on-LAN benötigen.
2. So aktivieren Sie **Acronis WOL Proxy** in den **Management Server-Optionen**:
   a. Aktivieren Sie das Kontrollkästchen **Folgende Proxies verwenden**.
   b. Klicken Sie auf **Hinzufügen** und geben Sie den Namen oder die IP-Adresse der Maschine ein, auf der der Acronis WOL Proxy installiert ist. Geben Sie die Anmeldedaten für die Maschine ein.
   c. Wiederholen Sie diesen Schritt, wenn es mehrere Acronis WOL Proxies gibt.
3. Aktivieren Sie beim Planen eines zentralen Backup-Plans die Einstellung **Wake-on-LAN verwenden**.

Sie können außerdem Proxies aus der Liste löschen. Denken Sie daran, dass jede Änderung dieser Option Auswirkungen auf den gesamten Management Server hat. Wenn Sie einen Proxy aus der Liste löschen, wird die Wake-on-LAN-Funktionalität im entsprechenden Subnetz für alle zentralen Backup-Pläne deaktiviert (einschließlich aller schon bereitgestellten).

15.4.10.2 Alarmmeldungen

Alarmverwaltung

Elemente von „Angenommene Alarmmeldungen“ entfernen, wenn älter als

Diese Option definiert, ob Meldungen aus der Tabelle für **Angenommene Alarmmeldungen** gelöscht werden sollen.

Voreinstellung ist: **Deaktiviert**.

Wenn aktiviert, können Sie für die angenommenen Alarmmeldungen einen Aufbewahrungszeitraum spezifizieren. Angenommene Alarmmeldungen, die älter als dieser Zeitraum sind, werden automatisch aus der Tabelle gelöscht.

Inaktive Alarmmeldungen automatisch zu „Angenommene Alarmmeldungen“ verschieben

Diese Option definiert, ob alle Alarmmeldungen, die inaktiv werden, angenommen und automatisch in die Tabelle **Angenommene Alarmmeldungen** verschoben werden sollen.

Voreinstellung ist: **Deaktiviert**.

Wenn aktiviert, können Sie die Alarmtypen spezifizieren, auf die diese Option angewendet wird.

Zeit-basierte Alarmmeldungen

Letztes Backup

Diese Option ist wirksam, wenn die Konsole zu einer verwalteten Maschine (S. 496) oder zum Management Server (S. 493) verbunden ist.

Die Option legt fest, ob eine Warnung erscheint, wenn auf der gegebenen Maschine nach Ablauf einer Zeitspanne kein Backup durchgeführt wurde. Sie können die Zeitspanne einrichten, die Sie als kritisch für Ihr Geschäftsumfeld betrachten.

Voreinstellung ist: Warnen, wenn die letzte erfolgreiche Sicherung auf einer Maschine vor mehr als **5 Tagen** vollendet wurde.

Der Alarm erscheint im Abschnitt **Warnungen** des **Dashboards**. Wenn die Konsole zum Management Server verbunden ist, wird diese Einstellung auch das Farbschema der Spalte **Letztes Backup** für jede Maschine steuern und wird auch .

Letzte Verbindung

Diese Option ist wirksam, wenn die Konsole zu einer verwalteten Maschine (S. 494) oder zum Management Server verbunden ist.

Die Option legt fest, ob eine Warnung erscheint, wenn innerhalb einer eingerichteten Zeitspanne keine Verbindung zwischen einer verwalteten Maschine und dem Management Server hergestellt wurde, die Maschine also möglicherweise nicht zentral verwaltet wurde (z.B. bei einem Ausfall der Netzverbindung zu dieser Maschine). Sie können die Zeitspanne festlegen, die als kritisch erachtet wird.

Voreinstellung ist: Warnen, wenn die letzte Verbindung der Maschine zum Management Server vor mehr als **5 Tagen** war.

Der Alarm erscheint im Abschnitt **Warnungen** des **Dashboards**. Wenn die Konsole zum Management Server verbunden ist, wird diese Einstellung auch das Farbschema der Spalte **Letzte Verbindung** für jede Maschine steuern und wird auch .

15.4.10.3 Domain-Zugriffsberechtigungen

Die Option bestimmt den vom Management Server verwendeten Benutzernamen und das Kennwort, um auf die Domain zuzugreifen.

Voreinstellung ist: Keine Anmeldedaten

Der Management Server benötigt Domain-Anmeldedaten, wenn er mit einer dynamischen Gruppe arbeitet, die auf dem **Organisationseinheit**-Kriterium (S. 419) basiert. Wenn Sie eine solche Gruppe erstellen und über diese Option keine Anmeldedaten angegeben werden, wird das Programm von Ihnen die Anmeldedaten erfragen und in dieser Option speichern.

Es ist ausreichend, die Anmeldedaten eines Benutzers zu spezifizieren, der Mitglied der Gruppe **Domain-Benutzer** auf der Domaine ist.

15.4.10.4 E-Mail-Einstellungen

Diese Option ermöglicht Ihnen E-Mail-Einstellungen zu konfigurieren, um Benachrichtigungen über auf dem Management Server aufgetretene Alarmmeldungen zu versenden.

Die Benachrichtigungsplanungen und Arten der zu versendenden Alarmmeldungen werden unter **Management Server-Optionen** –> **E-Mail-Einstellungen** –> **Alarmbenachrichtigungen** (S. 441) konfiguriert.

Voreinstellung ist: **Deaktiviert**.

Hinweis: *Alarmmeldungen warnen nur über Probleme. E-Mail-Benachrichtigungen über erfolgreiche Backup- und Recovery-Aktionen werden daher nicht versendet. Diese E-Mail-Benachrichtigungen werden unter Backup-Optionen –> Benachrichtigungen –> E-Mail (S. 131) bzw. unter Recovery-Optionen –> Benachrichtigungen –> E-Mail (S. 185) konfiguriert.*

So konfigurieren Sie eine E-Mail-Benachrichtigung

1. Geben Sie die E-Mail-Adresse des Ziels im Feld **E-Mail-Adressen** ein. Sie können auch mehrere, durch Semikolons getrennte Adressen eingeben.
2. Geben Sie in das Feld **Betreff** eine Beschreibung der Benachrichtigung ein oder lassen Sie den Wert leer. In dem Feld werden keine Variablen unterstützt.
3. Geben Sie im Feld **SMTP-Server** den Namen des ausgehenden Mail-Servers (SMTP) ein.
4. Legen Sie im Feld **Port** die Port-Nummer des ausgehenden Mail-Servers fest. Standardmäßig ist der Port auf **25** gesetzt.
5. Sollte der ausgehende Mail-Server eine Authentifizierung benötigen, dann geben Sie den **Benutzernamen** und das **Kennwort** vom E-Mail-Konto des Senders ein.

   Sollte der SMTP-Server keine Authentifizierung benötigen, dann lassen Sie die Felder **Benutzername** und **Kennwort** einfach leer. Falls Sie nicht sicher sind, ob Ihr SMTP-Server eine Authentifizierung erfordert, dann kontaktieren Sie Ihren Netzwerk-Administrator oder bitten Sie Ihren E-Mail-Dienstanbieter um Hilfe.
6. Klicken Sie auf **Erweiterte E-Mail-Parameter...**, um weitere E-Mail-Parameter folgendermaßen zu konfigurieren:
   a. **Von** – geben Sie den Namen des Absenders an. Falls Sie das Feld leer lassen, dann enthalten die Nachrichten im Feld **Von** das E-Mail-Konto des Senders.
   b. **Verschlüsselung verwenden** – Sie können sich für eine verschlüsselte Verbindung zum Mail-Server entscheiden. Zur Auswahl stehen die Verschlüsselungstypen SSL und TLS.
   c. Einige Internetdienstanbieter verlangen eine Authentifizierung am Posteingangsserver, bevor das Verschicken von Nachrichten erlaubt wird. Wenn das bei Ihnen zutrifft, aktivieren Sie das Kontrollkästchen **Anmeldung beim Posteingangsserver**, um einen POP3-Server zu aktivieren und seine Einstellungen einzurichten:
      - **Posteingangsserver (POP3)** – geben Sie den Namen des POP3-Servers an.
      - **Port** – bestimmt den Port des POP3-Servers. Standardmäßig ist der Port auf **110** gesetzt.
      - **Benutzername** und **Kennwort** für den eingehenden Mail-Server.
   d. Klicken Sie auf **OK**.
7. Klicken Sie auf **Test-Mail senden**, um zu überprüfen, ob die E-Mail-Benachrichtigungen mit den spezifizierten Einstellungen korrekt funktionieren.

Alarmbenachrichtigungen

Diese Option ermöglicht Ihnen festzulegen, wann E-Mail-Benachrichtigungen über auf dem Management Server aufgetretene Alarmmeldungen versendet werden sollen – und zudem festzulegen, welche Arten von Alarmmeldungen versendet werden sollen.

Stellen Sie bei Verwendung dieser Option sicher, dass die E-Mail-Benachrichtigungen unter **Management Server-Optionen** –> **E-Mail-Einstellungen** (S. 440) korrekt konfiguriert sind.

Voreinstellung ist: **Deaktiviert**.

So konfigurieren Sie die Alarmbenachrichtigungen

1. Wählen Sie, wann die Alarmbenachrichtigungen versendet werden sollen:
   - **Sobald ein Alarm auftritt** – um eine Benachrichtigung jedes Mal zu versenden, wenn ein neuer Alarm auftritt.

     Klicken Sie auf **Wählen Sie den Typ der Alarmmeldungen...**, um festzulegen, bei welcher Art von Alarm Benachrichtigungen versendet werden sollen.
   - **Benachrichtigung über alle aktuellen Alarmmeldungen nach Plan senden** – um eine gesammelte Alarmbenachrichtigung zu versenden, die alle Alarmmeldungen enthält, die in einer von Ihnen spezifizierten Zeitspanne aufgetreten sind.

     Klicken Sie auf **Wählen Sie den Typ der Alarmmeldungen...**, um festzulegen, bei welcher Art von Alarm Benachrichtigungen versendet werden sollen.

     Konfigurieren Sie die **Frequenz** und **Zeit** der Benachrichtigung.
2. Klicken Sie auf **OK**.

15.4.10.5 Ereignisverfolgung

Sie können den Management Server so konfigurieren, dass er die Ereignisse außer in seinem eigenen Log auch in der Ereignisanzeige von Windows protokolliert.

Sie können den Management Server so konfigurieren, dass er Simple Network Management Protocol (SNMP)-Objekte an einen spezifizierten SNMP-Manager sendet.

SNMP-Benachrichtigungen

Diese Option definiert, ob der Management Server seine eigenen Ereignis-Logs an spezifizierte Simple Network Management Protocol (SNMP)-Manager schicken muss. Sie können die Arten der Ereignisse wählen, die geschickt werden.

Zu weiteren Informationen über die Verwendung von SNMP mit Acronis Backup & Recovery 11.5 siehe „Unterstützung für SNMP (S. 56)".

Voreinstellung ist: **Deaktiviert**.

Versenden von SNMP-Benachrichtigungen einrichten

1. Aktivieren Sie das Kontrollkästchen **Meldungen an den SNMP-Server schicken**.
2. Spezifizieren Sie die passenden Optionen wie folgt:
   - **Ereignisse, die übermittelt werden** – Auswahl der Ereignistypen, die gesendet werden: **Alle Ereignisse**, **Fehler und Warnungen** oder **Nur Fehler**.
   - **Server-Name/IP** – Eintragen des Namens oder der IP-Adresse des Hosts mit der SNMP-Verwaltungsanwendung, an die die Meldungen gesendet werden.

- **Community** – Eintragen des Namens der SNMP-Community, zu der der Host mit der SNMP-Verwaltungsanwendung und die sendende Maschine gehören. Die typische Community ist „public“.

Klicken Sie auf **Testnachricht senden**, um die Richtigkeit der Einstellungen zu prüfen.

Um die Funktion auszuschalten, deaktivieren Sie das Kontrollkästchen **Meldungen an den SNMP-Server schicken**.

Die Nachrichten werden über UDP verschickt.

Ereignisanzeige von Windows

Diese Option definiert, ob der Management Server seine eigenen Ereignis-Logs in der Ereignisanzeige von Windows aufzeichnen muss. (Um die Ereignisanzeige zu sehen, führen Sie **eventvwr.exe** aus oder den Befehl **Systemsteuerung -> Verwaltung -> Ereignisanzeige**.) Sie können die Ereignisse filtern, die aufgezeichnet werden.

Voreinstellung ist: **Ausgeschaltet**.

Wählen Sie das Kontrollkästchen **Ereignisse protokollieren**, um diese Option einzuschalten.

Verwenden Sie das Kontrollkästchen **Ereignisse, die protokolliert werden**, um die Ereignisse zu filtern, die in der Ereignisanzeige von Windows aufgeführt werden:

- **Alle Ereignisse** – loggt alle Ereignisse (Informationen, Warnungen und Fehler)
- **Fehler und Warnungen**
- **Nur Fehler**.

Deaktivieren Sie das Kontrollkästchen **Ereignisse protokollieren**, um diese Option auszuschalten.

15.4.10.6 Aufzeichnungslevel

Diese Option legt fest, ob der Management Server das Log der Ereignisse auf den registrierten Maschinen im zentralen Log sammeln muss, das in einer zugeordneten Datenbank gespeichert wird und in der Ansicht **Log** zur Verfügung steht. Sie können die Option für alle Ereignisse auf einmal setzen oder die Ereignistypen auswählen, die gesammelt werden. Wenn Sie das Sammeln von Ereigniseinträgen vollständig deaktivieren, wird das zentrale Log nur das Log des Management Servers enthalten.

Voreinstellung ist: **Logs sammeln** für **Alle Ereignisse**.

Benutzen Sie das Listenfeld **Ereignisse, die protokolliert werden**, um die Art der Ereignisse anzugeben, die gesammelt werden:

- **Alle Ereignisse** – alle Ereignisse (Informationen, Warnungen und Fehler) der auf dem Management Server registrierten Maschinen werden in das zentrale Log eingetragen.
- **Fehler und Warnungen** – Warnungen und Fehler werden im zentralen Log aufgezeichnet.
- **Nur Fehler** – nur Fehler werden im zentralen Log aufgezeichnet.

Um das Sammeln der Ereignis-Logs auszuschalten, deaktivieren Sie das Kontrollkästchen **Logs sammeln**.

Log-Bereinigungsregeln

Diese Option spezifiziert, wie das zentrale Ereignis-Log bereinigt wird, das in der Berichtsdatenbank des Management Server gespeichert ist.

Diese Option definiert die maximale Größe der Berichtsdatenbank.

Voreinstellung ist: **Maximale Log-Größe: 1 GB**. **Bei Bereinigung, behalte 95% der maximalen Loggröße bei**.

Wenn diese Option aktiviert ist, vergleicht das Programm nach jeweils 100 Log-Einträgen die tatsächliche Log-Größe mit der maximalen Größe. Sobald die maximale Log-Größe überschritten ist, löscht das Programm die ältesten Log-Einträge. Sie können bestimmen, wie viele Log-Einträge beibehalten werden sollen. Mit der Standardeinstellung '95%' wird ein Großteil des Logs beibehalten. Mit der Minimaleinstellung '1%' wird das Log fast vollständig geleert.

Auch wenn Sie die Größenbeschränkung für das Log entfernen, werden ab einer Log-Größe von 4 GB keine weiteren Ereignisse in einer SQL Server Express Datenbank protokolliert, da die Datenbankgröße für die SQL Express Edition auf 4 GB beschränkt ist. Setzen Sie die maximale Log-Größe auf ca. 3,8 GB, um die maximale Größe der SQL Express Datenbank zu nutzen.

Diesen Parameter können Sie auch im Acronis Administrative Template (S. 453) setzen.

15.4.10.7 Online Backup-Proxy

Diese Option ist nur für Verbindungen zum Acronis Online Backup Storage über das Internet wirksam.

Diese Option bestimmt, ob sich der Management Server mit dem Internet über einen Proxy-Server verbinden soll.

Beachten Sie: *Acronis Backup & Recovery 11.5 unterstützt nur HTTP- und HTTPS-Proxy-Server.*

Die Proxy-Einstellungen für Agent und Management Server müssen separat konfiguriert werden, auch wenn sie auf derselben Maschine installiert sind.

So ändern Sie die Proxy-Server-Einstellungen

1. Aktivieren Sie das Kontrollkästchen **Einen Proxy-Server verwenden**.
2. Geben Sie unter **Adresse** den Netzwerknamen oder die IP-Adresse des Proxy-Servers an – beispielsweise: **proxy.beispielname.com** oder **192.168.0.1**
3. Spezifizieren Sie unter **Port** die Port-Nummer des Proxy-Servers – beispielsweise: **80**
4. Sollte der Proxy-Server eine Authentifizierung benötigen, dann geben Sie die entsprechenden Anmeldedaten unter **Benutzername** und **Kennwort** an.
5. Klicken Sie auf die Schaltfläche **Verbindung testen**, wenn Sie die Proxy-Server-Einstellungen überprüfen wollen.

15.5 Acronis Backup & Recovery 11.5-Komponenten konfigurieren

Es gibt drei Arten, die verschiedenen Parameter von Acronis Backup & Recovery 11.5-Komponenten in Windows zu konfigurieren:

- durch Verwendung des Acronis Administrative Template
- durch Verwendung der grafischen Benutzeroberfläche (GUI)
- durch Modifikation der Windows Registry

Unter Linux werden Parameter nicht durch Verwendung der administrativen Vorlage und Registry-Modifikation konfiguriert, sondern durch das Bearbeiten korrespondierender Konfigurationsdateien.

Falls die Werte eines per administrativer Vorlage gesetzten Parameters von denen abweichen, die per Benutzeroberfläche (GUI) gesetzt wurden, so erhalten die vorlagenbasierten Parameter Vorrang und werden sofort wirksam; die in der GUI angezeigten Werte werden dementsprechend abgeändert.

Die folgenden Abschnitte erläutern beide Arten der Konfiguration sowie die Parameter, die konfiguriert werden.

15.5.1 Per administrativen Template gesetzte Parameter

Der nachfolgende Abschnitt erläutert die Parameter der Acronis Backup & Recovery 11.5-Komponenten, die unter Verwendung des Acronis Administrative Template konfiguriert werden können. Zu Informationen, wie Sie die administrative Vorlage anwenden, siehe 'So laden Sie das Acronis Administrative Template (S. 444)'.

Das administrative Template enthält die Konfigurationsparameter des Acronis Backup & Recovery 11.5 Agenten, des Acronis Backup & Recovery 11.5 Management Servers, des Acronis Backup & Recovery 11.5 Storage Nodes sowie allgemeine Parameter der Acronis Backup & Recovery 11.5-Komponenten.

Die Parameter des Acronis Backup & Recovery 11.5 Storage Nodes sind im Abschnitt 'Storage Nodes (S. 254)' beschrieben. Die anderen Parameter sind in den entsprechenden Unterpunkten beschrieben.

15.5.1.1 So laden Sie das Acronis Administrative Template

Das von Acronis zur Verfügung gestellte administrative Template ermöglicht das Fein-Tuning einiger sicherheitsbezogener Funktionen, inklusive verschlüsselter Kommunikationseinstellungen. Durch den Microsoft Gruppenrichtlinien-Mechanismus können die Richtlinien-Einstellungen des Templates auf einen einzelnen Computer wie auch auf eine Domain angewendet werden.

So laden Sie das Acronis Administrative Template

1. Führen Sie den Editor für Windows Gruppenrichtlinienobjekte aus (%windir%\system32\gpedit.msc).
2. Öffnen Sie das zur Bearbeitung gewünschte Gruppenrichtlinienobjekt (Group Policy object, GPO).
3. Erweitern Sie den Ast **Computerkonfiguration**.
4. Klicken Sie mit der rechten Maustaste auf **Administratives Template**.
5. Klicken Sie auf **Template hinzufügen/entfernen**.
6. Klicken Sie auf **Hinzufügen**.
7. Gehen Sie zu 'Acronis Administrative Template' und klicken Sie auf **Öffnen**. Der Pfad zum administrativen Template ist:
   - Unter einer 32-Bit-Version von Windows: **%CommonProgramFiles%\Acronis\Agent\Acronis_agent.adm** oder **%ProgramFiles%\Acronis\BackupAndRecoveryConsole\Acronis_agent.adm**
   - Unter einer 64-Bit-Version von Windows: **%CommonProgramFiles(x86)%\Acronis\Agent\Acronis_agent.adm** oder **%ProgramFiles(x86)%\Acronis\BackupAndRecoveryConsole\Acronis_agent.adm**

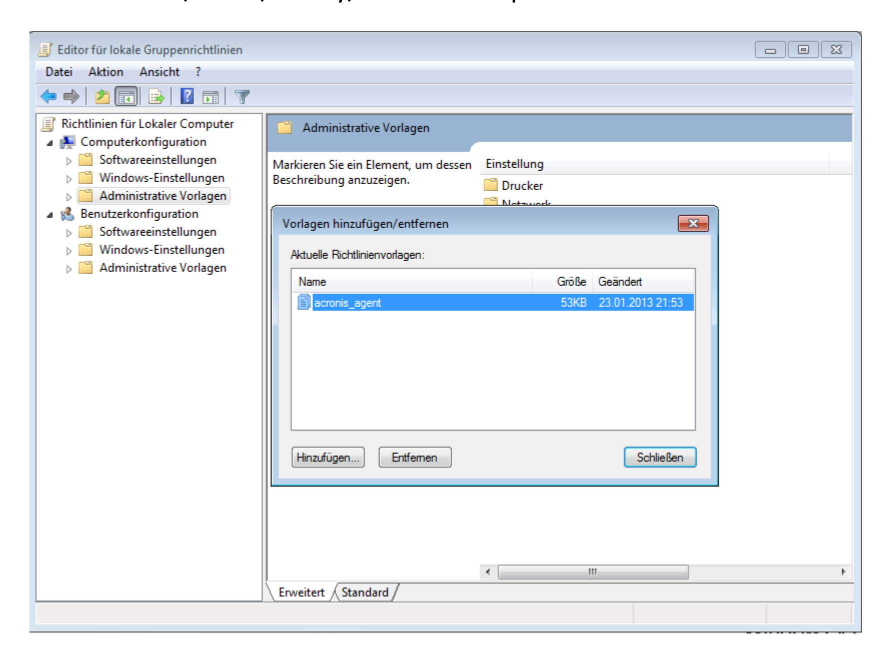
Sobald das Template geladen wurde, können Sie es öffnen und gewünschte Einstellungen bearbeiten. Nachdem Sie das Template geladen oder dessen Einstellungen bearbeitet haben, sollten Sie die konfigurierten Komponente(n) oder einige ihrer Dienste neu starten.

Zu detaillierten Informationen über den Windows Gruppenrichtlinien-Editor siehe:

http://msdn2.microsoft.com/en-us/library/aa374163.aspx

Zu detaillierten Informationen über Gruppenrichtlinien siehe:

http://msdn2.microsoft.com/en-us/library/aa374177.aspx



15.5.1.2 Acronis Backup & Recovery 11.5

Dieser Abschnitt der administrativen Vorlage spezifiziert die Verbindungsparameter und Parameter zur Ereignisverfolgung für die nachfolgenden Acronis Backup & Recovery 11.5-Komponenten:

- Acronis Backup & Recovery 11.5 Management Server
- Acronis Backup & Recovery 11.5 Agent
- Acronis Backup & Recovery 11.5 Storage Node

Verbindungsparameter

Ports für Remote Agent

Spezifiziert den Port, den die Komponente für eingehende und ausgehende Kommunikation mit anderen Acronis-Komponenten verwendet.

Wählen Sie eine der nachfolgenden Varianten:

Nicht konfiguriert

Die Komponente wird den Standard-TCP-Port mit der Nummer 9876 verwenden.

Aktiviert

Die Komponente wird den angegebenen Port verwenden; geben Sie die entsprechende Port-Nummer in das Feld **Server TCP-Port** ein.

Deaktiviert

Gleichbedeutend mit **Nicht konfiguriert**.

Optionen für Client-Verschlüsselung

Spezifiziert, ob eine verschlüsselte Datenübertragung erfolgt, sofern die Komponente als Client-Applikation agiert, und ob selbst-signierten SSL-Zertifikaten vertraut wird.

Wählen Sie eine der nachfolgenden Varianten:

Nicht konfiguriert

Die Komponente wird die Standardeinstellungen verwenden, also möglichst mit Verschlüsselung zu arbeiten und selbst-signierten SSL-Zertifikaten zu vertrauen (siehe die nachfolgende Option).

Aktiviert

Verschlüsselung ist eingeschaltet. Wählen Sie bei **Verschlüsselung** Folgendes:

Aktiviert

Die Datenübertragung erfolgt verschlüsselt, falls auch bei der Server-Applikation die Verschlüsselung eingeschaltet ist, anderenfalls bleibt die Übertragung unverschlüsselt.

Deaktiviert

Verschlüsselung ist ausgeschaltet – es werden keine Verbindungen zu Server-Applikationen aufgebaut, die eine Verschlüsselung erfordern.

Erforderlich

Die Datenübertragung erfolgt verschlüsselt, wird aber nur aufgebaut, falls bei der Server-Applikation die Verschlüsselung aktiviert ist (siehe „Optionen für Server-Verschlüsselung“).

Parameter zur Authentifizierung

Eine Aktivierung des Kontrollkästchens **Selbst-signierten Zertifikaten vertrauen** erlaubt dem Client, sich mit einer Server-Applikation zu verbinden, die selbst-signierte SSL-Zertifikate benutzt (wie solche Zertifikate, die während der Installation von Acronis Backup & Recovery 11.5-Komponenten erstellt wurden) — siehe SSL-Zertifikate (S. 394).

Sie sollten dieses Kontrollkästchen aktiviert lassen, außer Sie verwenden in Ihrem Umfeld eine Public Key-Infrastruktur (PKI).

Wählen Sie Folgendes in **Verwende Agent-Zertifikatsauthentifizierung**:

Nicht verwenden

Die Verwendung von SSL-Zertifikaten ist deaktiviert. Zu Server-Applikationen, die die Verwendung von SSL-Zertifikaten erfordern, werden keine Verbindungen aufgebaut.

Verwende wenn möglich

Die Verwendung von SSL-Zertifikaten ist aktiviert. Der Client wird SSL-Zertifikate nutzen, sofern ihre Verwendung auch bei der Server-Applikation eingeschaltet ist – anderenfalls werden sie nicht verwendet.

Immer verwenden

Die Verwendung von SSL-Zertifikaten ist aktiviert. Die Verbindung wird nur dann aufgebaut, wenn die Verwendung von SSL-Zertifikaten auch auf der Server-Applikation eingeschaltet ist.

Deaktiviert

Gleichbedeutend mit **Nicht konfiguriert**.

Optionen für Server-Verschlüsselung

Spezifiziert, ob die Datenübertragung verschlüsselt erfolgen soll, wenn die Komponente als Server-Applikation agiert.

Wählen Sie eine der nachfolgenden Varianten:

Nicht konfiguriert

Die Komponente wird die Standardeinstellung verwenden, welche „verwende Verschlüsselung wenn möglich“ ist (siehe nachfolgende Option).

Aktiviert

Verschlüsselung ist eingeschaltet. Wählen Sie bei **Verschlüsselung** Folgendes:

Aktiviert

Die Datenübertragung erfolgt verschlüsselt, falls auch bei der Client-Applikation die Verschlüsselung eingeschaltet ist, anderenfalls bleibt die Übertragung unverschlüsselt.

Deaktiviert

Verschlüsselung ist deaktiviert; es werden keine Verbindungen zu Client-Applikationen aufgebaut, die eine Verschlüsselung erfordern.

Erforderlich

Die Datenübertragung erfolgt verschlüsselt, wird aber nur aufgebaut, falls bei der Client-Applikation die Verschlüsselung aktiviert ist (siehe „Optionen für Client-Verschlüsselung“).

Parameter zur Authentifizierung

Wählen Sie Folgendes in **Verwende Agent-Zertifikatsauthentifizierung**:

Nicht verwenden

Die Verwendung von SSL-Zertifikaten ist deaktiviert. Zu Client-Applikation, die die Verwendung von SSL-Zertifikaten erfordern, werden keine Verbindungen aufgebaut.

Verwende wenn möglich

Die Verwendung von SSL-Zertifikaten ist aktiviert. Der Server wird SSL-Zertifikate nutzen, sofern ihre Verwendung auch bei der Client-Applikation eingeschaltet ist – anderenfalls werden sie nicht verwendet.

Immer verwenden

Die Verwendung von SSL-Zertifikaten ist aktiviert. Die Verbindung wird nur dann aufgebaut, wenn die Verwendung von SSL-Zertifikaten auch auf der Client-Applikation eingeschaltet ist.

Deaktiviert

Gleichbedeutend mit **Nicht konfiguriert**.

Parameter für die Ereignisverfolgung

In Windows können Ereignisse, die in Acronis Backup & Recovery 11.5 auftreten, in der Ereignisanzeige, in eine Datei oder beides aufgezeichnet werden.

Jedes Ereignis hat ein Level von Null bis Fünf, basierend auf dem Schweregrad des Ereignisses – wie in der nachfolgenden Tabelle aufgelistet:

Level	Name	Beschreibung
0	Unbekannt	Ereignis, dessen Schweregrad unbekannt oder nicht zutreffend ist
1	Debug	Für Debug-Zwecke verwendetes Ereignis
2	Informationen	Informierendes Ereignis, wie etwa über den erfolgreichen Aktionsabschluss oder Start eines Dienstes
3	Warnung	Ereignis, das ein möglicherweise bevorstehendes Problem ist, wie etwa zu wenig freier Platz in einem Depot
4	Fehler	Ereignis, das zum Verlust von Daten oder Funktionalität führte
5	Kritisch	Ereignis, das zum Abbruch eines Prozesses (z.B. Prozess des Agenten) führte

Ereignis-verfolgende Parameter werden über folgende Einstellungen im administrativen Template spezifiziert:

File Trace Minimal Level

Beschreibung: Spezifiziert den niedrigsten Schweregrad, ab dem Ereignisse in die Datei aufgezeichnet werden. Nur Ereignisse mit Leveln größer oder gleich zu **File Trace Minimal Level** werden aufgezeichnet.

Mögliche Werte: Jeder Schweregrad von **Unbekannt** bis **Kritisch** oder **Blockiert**, um überhaupt keine Ereignisse aufzuzeichnen

Standardwert: 2 (Ereignisse mit Schweregrad 2 bis 5 werden aufgezeichnet)

Die Log-Dateien befinden sich innerhalb des Ordners **%ALLUSERSPROFILE%\Application Data\Acronis** (in Windows XP und Server 2003) oder **%PROGRAMDATA%\Acronis** (in Windows Vista und späteren Versionen von Windows) – und dort im Unterordner **Logs** der jeweiligen Komponente.

Win32 Trace Minimal Level

Beschreibung: Spezifiziert den niedrigsten Schweregrad, ab dem Ereignisse in der Ereignisanzeige des Systems aufgezeichnet werden. Nur Ereignisse mit Leveln größer oder gleich zu **Win32 Trace Minimal Level** werden aufgezeichnet.

Mögliche Werte: Jeder Schweregrad von **Unbekannt** bis **Kritisch** oder **Blockiert**, um überhaupt keine Ereignisse aufzuzeichnen

Standardwert: 4 (Ereignisse über Fehler und kritische Fehler werden aufgezeichnet)

Programm zur Kundenzufriedenheit (CEP)

Spezifiziert, ob die Maschine, auf der die Acronis Backup & Recovery 11.5-Komponente installiert wird, am Programm zur Kundenzufriedenheit (CEP) teilnimmt.

Wählen Sie eine der nachfolgenden Varianten:

Nicht konfiguriert

Standardmäßig nimmt die Maschine nicht am Programm zur Kundenzufriedenheit (CEP) teil.

Aktiviert

Wählen Sie unter **Ermögliche, Berichte an Acronis zu senden** eine der folgenden Optionen:

Aktivieren

Auf der Maschine werden Informationen gesammelt (über die Hardware-Konfiguration, am häufigsten und am wenigsten verwendete Funktionen, sowie Probleme) und regelmäßig an Acronis geschickt. Die Ergebnisse sind dazu gedacht, Verbesserungen bei der Software und Funktionalität zu ermöglichen, um die Bedürfnisse von Acronis-Kunden noch besser zu erfüllen. Acronis sammelt keine persönliche Daten. Die Teilnahmebedingungen können auf der Acronis-Website gefunden werden.

Deaktivieren

Es wird keine Information verschickt.

Deaktiviert

Gleichbedeutend mit **Nicht konfiguriert**.

15.5.1.3 Acronis Backup & Recovery 11.5 Agent für Windows

Der nachfolgende Abschnitt erläutert die Parameter des Acronis Backup & Recovery 11.5-Agenten, die unter Verwendung des Acronis Administrative Template konfiguriert werden können.

Lizenzierung

Spezifiziert, wie oft der Agent seine Lizenz auf dem License Server überprüft und wie lange er ohne einen License Server arbeiten kann.

License Check Interval (in Tagen)

Beschreibung: Spezifiziert, wie oft (in Tagen) nach Lizenz-Verfügbarkeit auf dem Acronis License Server geprüft werden soll.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **5**

Standardwert: **1**

Der Acronis Backup & Recovery 11.5 Agent überprüft periodisch, ob sein Lizenzschlüssel auf dem License Server vorhanden ist. Die erste Überprüfung wird jedes Mal durchgeführt, wenn der Acronis Backup & Recovery 11.5 Agent startet, weitere Überprüfungen erfolgen dann je einmal in der Zahl von Tagen, die unter **License Check Interval** angegeben wurden.

Eine Warnung wird in die Ereignisanzeige des Agenten aufgenommen, wenn er sich nicht mit dem License Server verbinden kann. Sie können die Warnung im Dashboard einsehen.

Wenn der Wert **0** beträgt, wird keine Lizenzprüfung durchgeführt; ohne Lizenz wird die Funktionalität von Acronis Backup & Recovery 11.5 nach der Zahl von Tagen deaktiviert, die unter **Maximum Time without License Server** vorgegeben wurde (siehe nächsten Parameter).

Siehe auch **License Server Connection Retry Interval** weiter unten in diesem Abschnitt.

Maximum Time without License Server (in Tagen)

Beschreibung: Spezifizieren Sie, wie viele Tage Acronis Backup & Recovery 11.5 normal arbeiten wird, bis seine Funktionalität deaktiviert wird.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **60**

Standardwert: **30**

Falls der Acronis License Server nicht verfügbar ist, wird Acronis Backup & Recovery 11.5 für die Zahl an Tagen mit voller Funktionalität weiterarbeiten, wie unter **Maximum Time without License Server** spezifiziert – gezählt vom Beginn der Installation oder von der letzten erfolgreichen Überprüfung.

License Server Connection Retry Interval (in Stunden)

Beschreibung: Spezifiziert das Intervall, in Stunden, zwischen zwei Verbindungsversuchen, falls der Acronis License Server nicht verfügbar ist.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **24**

Standardwert: **1**

Falls während einer Lizenzschlüssel-Überprüfung (siehe **License Check Interval**, weiter oben in diesem Abschnitt) der Acronis Backup & Recovery 11.5 Agent sich nicht mit dem License Server verbinden konnte, so wird er dies je einmal innerhalb der Zahl an Stunden erneut versuchen, wie sie über **License Server Connection Retry Interval** vorgegeben wurden.

Sollte der Wert **0** betragen, so erfolgen keine erneuten Verbindungsversuche, der Agent überprüft stattdessen die Lizenz nur noch wie durch **License Check Interval** bestimmt.

License Server Address

Beschreibung: Spezifiziert den Netzwerknamen oder die IP-Adresse des Acronis License Servers.

*Mögliche Werte:*Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: Leere Zeichenfolge

Log-Bereinigungsregeln

Spezifiziert, wie das Log das Agenten bereinigt wird.

Dieser Parameter hat die folgenden Einstellungen:

Maximale Größe

Beschreibung: Spezifiziert die maximale Größe des Log-Ordners des Agenten in Kilobyte.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **2.147.483.647**

Standardwert: **1048576** (1 GB)

Zu erhaltender Anteil

Beschreibung: Spezifiziert die maximale Log-Größe in Prozent, die bei der Bereinigung zu erhalten ist.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **100**

Standardwert: **95**

Details zur Bereinigung des Agent-Logs finden Sie unter Log-Bereinigungsregeln (S. 383).

Windows Event Log

Spezifiziert, wann Ereignisse von Acronis Backup & Recovery 11.5 Agent in der Ereignisanzeige von Windows aufgezeichnet werden.

Dieser Parameter hat zwei Einstellungen:

Trace State

Beschreibung: Spezifiziert, ob die Ereignisse des Agenten in das Ereignis-Log aufgenommen werden sollen.

Mögliche Werte: **Aktiviert** oder **Deaktiviert**

Standardwert: **Aktiviert**

Trace Level

Beschreibung: Spezifiziert den minimalen Schweregrad von Ereignissen, damit diese in das Ereignis-Log aufgenommen werden. Nur Ereignisse mit Leveln größer oder gleich zu den unter **Trace Level** angegebenen Werten werden gesammelt.

Mögliche Werte: **0** (internes Ereignis), **1** (Debugging-Information), **2** (Information), **3** (Warnung), **4** (Fehler) oder **5** (kritischer Fehler)

Standardwert: **4** (nur Fehler und kritische Fehler werden gesendet — falls **Trace State**auf **Aktiviert** gesetzt ist)

SNMP

Spezifiziert die Art der Ereignisse des Agenten, über die Benachrichtigungen mit Hilfe des Simple Network Management Protocols (SNMP) verschickt werden sollen.

Dieser Parameter hat die folgenden Einstellungen:

Trace State

Beschreibung: Spezifiziert, ob SNMP-Benachrichtigungen verschickt werden sollen.

Mögliche Werte: **Aktiviert** oder **Deaktiviert**

Standardwert: **Aktiviert**

Trace Level

Beschreibung: Spezifiziert den minimalen Schweregrad der Ereignisse, damit SNMP-Benachrichtigungen über diese verschickt werden. Nur Benachrichtigungen über Ereignisse, deren Schweregrad größer oder gleich zu **Trace Level** ist, werden versendet.

Mögliche Werte: **0** (internes Ereignis), **1** (Debugging-Information), **2** (Information), **3** (Warnung), **4** (Fehler) oder **5** (kritischer Fehler)

Standardwert: **4** (nur Fehler und kritische Fehler werden gesendet — falls **Trace State**auf **Aktiviert** gesetzt ist)

SNMP-Adresse

Beschreibung: Spezifiziert den Netzwerknamen oder die IP-Adresse des SNMP-Servers.

*Mögliche Werte:*Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: Leere Zeichenfolge

SNMP-Community

Beschreibung: Spezifiziert den Community-Namen für die SNMP-Benachrichtigungen.

*Mögliche Werte:*Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: **öffentlich**

Snapshot Storage

Spezifiziert den Ort und die Anfangsgröße des Storages für Snapshots – eine temporäre Datei, die beim Backup der Daten durch einen Snapshot benutzt wird. Die Datei wird gelöscht, sobald das Backup vollständig ist.

Mit den Standardeinstellungen wird der Snapshot-Storage im Ordner für temporäre Dateien des Agenten erstellt und belegt anfänglich 20 Prozent vom verfügbaren Speicherplatze des Volumes, das diesen Ordner enthält. Es wird mehr Platz verwendet, wenn das für den Snapshot erforderlich ist.

Sie können die Anfangsgröße für den Snapshot-Storage erhöhen – oder diesen auf ein anderes Volume verlegen – wenn Probleme mit dem Backup von Daten auftreten, die sich während des Backups umfangreich ändern.

Dieser Parameter wird bei Erstellung eines lokalen Backup-Plans verwendet. Änderungen an diesem Parameter haben keinen Einfluss auf bereits existierende lokale Backup-Pläne.

Dieser Parameter hat die folgenden Einstellungen:

Pfad zum Snapshot-Ordner

Beschreibung: Spezifiziert das Verzeichnis, in dem der Snapshot-Storage erstellt wird.

*Mögliche Werte:*Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: Leere Zeichenfolge

Eine leere Zeichenfolge entspricht dem Ordner '%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\MMS\Temp' (in Windows XP und Server 2003) oder '%PROGRAMDATA%\Acronis\BackupAndRecovery\MMS\Temp' (in Windows Vista und späteren Versionen von Windows).

Sie können einen lokalen Ordner auf einem beliebigen Volume angeben, einschließlich eines Volumes, das Sie sichern.

Pre-allocated storage size (in Megabyte)

Beschreibung: Spezifiziert die Anfangsgröße des Snapshot-Storages in Megabyte.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **2.147.483.647**

Standardwert: **0**

Lautet die Einstellung **0**, dann verwendet der Management Server die Einstellung **Pre-allocated storage size (in Prozent)**.

Die Anfangsgröße wird den verfügbaren Platz abzüglich 50 MB nicht überschreiten.

Pre-allocated storage size (in Prozent)

Diese Einstellung ist nur wirksam, wenn die Einstellung **Pre-allocated storage size (in Megabyte)** den Wert **0** hat.

Beschreibung: Spezifiziert die Anfangsgröße des Snapshot-Storages als Prozentwert des Festplattenplatzes, der zum Zeitpunkt des Backup-Starts zur Verfügung steht.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **100**

Standardwert: **50**

Beträgt der Wert **0**, dann wird kein Snapshot-Storage erstellt.

Die Anfangsgröße wird den verfügbaren Platz abzüglich 50 MB nicht überschreiten.

Die Erstellung von Snapshots ist auch ohne Snapshot-Storage möglich.

Die Größe des Snapshot-Storages beeinflusst die Größe des Backups nicht.

Online Backup-Proxy

Spezifiziert die Proxy-Server-Einstellungen für Internetverbindungen zum Acronis Online Backup Storage.

Dieser Parameter hat die folgenden Einstellungen:

Proxy

Beschreibung: Spezifiziert, ob ein Proxy-Server verwendet werden soll.

Mögliche Werte: **Aktiviert** oder **Deaktiviert**

Standardwert: **Aktiviert**

Falls der Wert dieses Parameters **deaktiviert** ist, werden alle nachfolgenden Parameter ignoriert.

Adresse des Proxy-Servers

Beschreibung: Spezifiziert den Namen oder die IP-Adresse des Proxy-Servers

*Mögliche Werte:*Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: Leere Zeichenfolge

Port des Proxy-Servers

Beschreibung: Spezifiziert die Port-Nummer des Proxy-Servers

*Mögliche Werte:*Jede ganze Zahl zwischen 0 und 65535

Standardwert: **0**

Anmeldedaten für den Online Backup-Proxy

Verwenden Sie folgende zwei Parameter, falls der Proxy-Server zur Verbindung mit dem Acronis Online Backup Storage eine Authentifizierung erfordert.

Benutzername

Beschreibung: Spezifiziert den Benutzernamen zur Authentifizierung am Proxy-Server

*Mögliche Werte:*Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: Leere Zeichenfolge

Kennwort

Beschreibung: Spezifiziert das Kennwort zur Authentifizierung am Proxy-Server

*Mögliche Werte:*Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: Leere Zeichenfolge

Wichtig. Das Kennwort kann von jedem Benutzer eingesehen werden, der Zugriff auf das administrative Template hat – wie etwa ein Administrator der Maschine.

Katalogisierung

Beschreibung: Spezifiziert, ob der Acronis Backup & Recovery 11.5 Agent Backups in nicht verwalteten Depots katalogisieren wird.

Mögliche Werte: **Aktiviert** (katalogisieren) oder **Deaktiviert** (nicht katalogisieren)

Standardwert: **Aktiviert**

Falls der Wert dieses Parameters **Deaktiviert** ist, wird die **Datenanzeige** keine Daten für ein Depot anzeigen, wenn die Management Konsole direkt mit der Maschine verbunden ist.

Maschinen-Neustart bei laufenden Tasks unterdrücken

Beschreibung: Spezifiziert, was passieren soll, falls die Maschine während einer Task-Ausführung ausgeschaltet oder neu gestartet werden muss.

Mögliche Werte: **Aktiviert** (warten, bis der Task beendet ist) oder **Deaktiviert** (den Task stoppen)

Standardwert: **Deaktiviert**

15.5.1.4 Acronis Backup & Recovery 11.5 Management Server

Der nachfolgende Abschnitt erläutert die Parameter des Acronis Backup & Recovery 11.5 Management Server, die unter Verwendung des Acronis Administrative Template konfiguriert werden können.

Collecting Logs

Spezifiziert, wann Log-Einträge von Maschinen gesammelt werden, die durch den Acronis Backup & Recovery 11.5 Management Server verwaltet werden.

Dieser Parameter enthält zwei Einstellungen:

Trace State

Beschreibung: Spezifiziert, ob Log-Einträge über die Ereignisse der Komponenten auf den registrierten Maschinen erfasst werden sollen.

Mögliche Werte: **Aktiviert** oder **Deaktiviert**

Standardwert: **Aktiviert**

Trace Level

Beschreibung: Spezifiziert den minimalen Schweregrad der gesammelten Einträge. Nur Einträge mit Leveln größer oder gleich zu den unter **Trace Level** angegebenen Werten werden gesammelt.

Mögliche Werte: **0** (internes Ereignis), **1** (Debugging-Information), **2** (Information), **3** (Warnung), **4** (Fehler) oder **5** (kritischer Fehler)

Standardwert: **0** (alle Einträge werden gesammelt)

Log-Bereinigungsregeln

Spezifiziert, wie das zentrale Ereignis-Log bereinigt wird, das in der Berichtsdatenbank des Management Servers gespeichert ist.

Dieser Parameter hat die folgenden Einstellungen:

Maximale Größe

Beschreibung: Spezifiziert die maximale Größe des zentralen Ereignis-Logs in Kilobyte.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **2.147.483.647**

Standardwert: **1048576** (1 GB)

Zu erhaltender Anteil

Beschreibung: Spezifiziert die maximale Log-Größe in Prozent, die bei der Bereinigung zu erhalten ist

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **100**

Standardwert: **95**

Details zur Bereinigung des zentralen Ereignis-Logs finden Sie unter Log-Bereinigungsregeln (S. 442).

Windows Event Log

Spezifiziert, wann Ereignisse von Acronis Backup & Recovery 11.5 Management Server in der Ereignisanzeige von Windows aufgezeichnet werden.

Dieser Parameter hat zwei Einstellungen:

Trace State

Beschreibung: Spezifiziert, ob die Ereignisse des Acronis Backup & Recovery 11.5 Management Servers im Ereignis-Log aufgezeichnet werden sollen.

Mögliche Werte: **Aktiviert** oder **Deaktiviert**

Standardwert: **Aktiviert**

Trace Level

Beschreibung: Spezifiziert den minimalen Schweregrad von Ereignissen, damit diese in das Ereignis-Log aufgenommen werden. Nur Ereignisse mit Leveln größer oder gleich zu den unter **Trace Level** angegebenen Werten werden gesammelt.

Mögliche Werte: **0** (internes Ereignis), **1** (Debugging-Information), **2** (Information), **3** (Warnung), **4** (Fehler) oder **5** (kritischer Fehler)

Standardwert: **4** (nur Fehler und kritische Fehler werden gesendet — falls **Trace State**auf **Aktiviert** gesetzt ist)

SNMP

Spezifiziert die Art der Ereignisse des Management Servers, über die Benachrichtigungen mit Hilfe des Simple Network Management Protocols (SNMP) verschickt werden sollen.

Dieser Parameter enthält folgende Einstellungen:

Trace State

Beschreibung: Spezifiziert, ob SNMP-Benachrichtigungen verschickt werden sollen.

Mögliche Werte: **Aktiviert** oder **Deaktiviert**

Standardwert: **Aktiviert**

Trace Level

Beschreibung: Spezifiziert den minimalen Schweregrad der Ereignisse, damit SNMP-Benachrichtigungen über diese verschickt werden. Nur Benachrichtigungen über Ereignisse, deren Schweregrad größer oder gleich zu **Trace Level** ist, werden versendet.

Mögliche Werte: **0** (internes Ereignis), **1** (Debugging-Information), **2** (Information), **3** (Warnung), **4** (Fehler) oder **5** (kritischer Fehler)

Standardwert: **4** (nur Fehler und kritische Fehler werden gesendet — falls **Trace State**auf **Aktiviert** gesetzt ist)

SNMP-Adresse

Beschreibung: Spezifiziert den Netzwerknamen oder die IP-Adresse des SNMP-Servers.

*Mögliche Werte:*Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: Leere Zeichenfolge

SNMP-Community

Beschreibung: Spezifiziert den Community-Namen für die SNMP-Benachrichtigungen.

*Mögliche Werte:*Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: **öffentlich**

Synchronisierung

Spezifiziert, wie sich der Acronis Backup & Recovery 11.5 Management Server mit den registrierten Maschinen verbindet, um zentrale Backup-Pläne bereitzustellen, Logs und Backup-Plan-Zustände abzufragen und ähnliche Aktionen auszuführen – zusammenfassend 'Synchronisierung' genannt.

Dieser Parameter hat die folgenden Einstellungen:

Maximum Connections

Beschreibung: Spezifiziert die maximale Zahl gleichzeitiger Synchronisierungsverbindungen, die aufrechterhalten werden sollen.

*Mögliche Werte:*Jede ganze Zahl zwischen **1** und **500**

Standardwert: **200**

Solange die Gesamtzahl online registrierter Maschinen den unter **Maximum Connections** angegebenen Wert nicht überschreitet, wird die Verbindung zu diesen Maschinen immer aufrechterhalten und führt der Management Server mit jeder Maschine periodische Synchronisierungen aus.

Im anderen Fall verbindet er sich mit der Zahl von registrierten Maschinen, die der zugewiesenen Anzahl gleichzeitiger Verbindungen entspricht. Wurde die Synchronisierung für eine Maschine abgeschlossen, so trennt sich der Management Server von dieser und nutzt die freigewordene Verbindung zur Synchronisierung mit einer weiteren Maschine und so weiter.

(Hinweis: Verbindungen zu Maschinen mit hoher Synchronisierungspriorität — siehe **Periode-High Priority** später in diesem Abschnitt — werden voraussichtlich immer aufrechterhalten.)

Synchronisierungsverbindungen haben nichts mit den Verbindungen zu tun, wie sie zwischen Acronis Backup & Recovery 11.5 Management Server und der Acronis Backup & Recovery 11.5 Management Console erfolgen.

Maximum Workers

Beschreibung: Spezifiziert die maximale Zahl von Threads, die zur Synchronisierung verwendet werden sollen.

*Mögliche Werte:*Jede ganze Zahl zwischen **1** und **100**

Standardwert: **30**

Der Prozess des Management Servers nutzt spezielle Threads – auch Arbeits-Threads genannt – um die Synchronisierung mit einer registrierten, verbundenen Maschine durchzuführen.

Jeder Arbeits-Thread führt die Synchronisierung nur mit je einer Maschine gleichzeitig aus.

Eine zur Synchronisierung verbundene Maschine wartet auf einen verfügbaren Arbeits-Thread. Daher wird die tatsächliche Zahl von Arbeits-Threads nie die maximale Zahl von Verbindungen überschreiten (siehe **Maximum Connections**, wie zuvor beschrieben).

Periode (in Sekunden)

Beschreibung: Spezifiziert, wie oft (in Sekunden) die Synchronisierung für Maschinen, die eine normale Synchronisierungspriorität haben, durchgeführt wird – typischerweise Maschinen ohne aktuell ausgeführte, zentrale Backup-Tasks.

*Mögliche Werte:*Jede ganze Zahl zwischen **120** und **2.147.483.647**

Standardwert: **120**

Der Acronis Backup & Recovery 11.5 Management Server versucht die Synchronisierung für jede Maschine mit normaler Priorität je einmal innerhalb des Zeitraums durchzuführen, der

in Sekunden über **Period** vorgegeben wurde – wobei er je einen verfügbaren Arbeits-Thread verwendet (siehe **Maximum Workers**, wie zuvor beschrieben).

Sollte es weniger Arbeits-Threads als Maschinen mit normaler Priorität geben, so kann das tatsächliche Intervall zwischen den Synchronisierungen länger als der angegebene Wert des Parameters sein.

Period-High Priority (in Sekunden)

Beschreibung: Spezifiziert, wie oft (in Sekunden) die Synchronisierung für Maschinen, die eine hohe Synchronisierungspriorität haben, durchgeführt wird – typischerweise Maschinen mit aktuell ausgeführten, zentralen Backup-Tasks.

*Mögliche Werte:*Jede ganze Zahl zwischen **15** und **2.147.483.647**

Standardwert: **15**

Dieser Parameter ist analog zu dem eben beschriebenen Parameter **Period**.

Real-Time Monitoring

Beschreibung: Spezifiziert, ob ein Echtzeit-Monitoring von registrierten Maschinen durchgeführt werden soll, statt einen Polling-Mechanimus zu verwenden.

Mögliche Werte: **Aktiviert** oder **Deaktiviert**

Standardwert: **Deaktiviert**

Standardmäßig ist es der Acronis Backup & Recovery 11.5 Management Server, der sich mit den registrierten Maschinen verbindet, um eine Synchronisierung durchzuführen – insbesondere, um Daten wie Backup-Logs abzurufen. Dieser Ansatz ist auch als Polling-Mechanismus bekannt.

Falls jedoch **Real Time Monitoring** auf **Aktiviert** gesetzt ist, sendet der Management Server stattdessen Anfragen an die Maschinen, neue Daten anzubieten, wenn diese auftauchen bzw. entstehen – und geht dann in einen Lauschmodus. Dieser Ansatz wird Echtzeit-Monitoring genannt.

Echtzeit-Monitoring kann den Netzwerkverkehr reduzieren – z.B. wenn zentrale Backup-Tasks selten ablaufen. Es ist jedoch nur dann effektiv, wenn es relativ wenig registrierte Maschinen gibt.

Vermeiden Sie es, Echtzeit-Monitoring zu aktivieren, wenn die Zahl an registrierten Maschinen die maximale Zahl gleichzeitiger Verbindungen übersteigt (siehe **Maximum Connections**, weiter oben in diesem Abschnitt).

Zweiter Verbindungsversuch

Beschreibung: Spezifiziert, ob ein erneuter Verbindungsversuch zu einer registrierten Maschine unternommen werden soll, indem die letztbekannte IP-Adresse verwendet wird, nachdem ein Verbindungsversuch unter Verwendung des Host-Namens gescheitert ist.

Mögliche Werte: **Aktiviert** oder **Deaktiviert**

Standardwert: **Deaktiviert**

Der Acronis Backup & Recovery 11.5 Management Server verwendet beim Verbindungsversuch mit einer registrierten Maschine zuerst ihren Netzwerknamen – vorausgesetzt die Maschine wurde dem Management Server über ihren Namen hinzugefügt.

Falls der Parameter **Second Connection Attempt** auf **Aktiviert** eingestellt ist und eine Verbindung zur Maschine unter Verwendung ihres Netzwerknamens gescheitert ist, so macht der Management Server einen zweiten Verbindungsversuch, indem er diesmal die letzte IP-Adresse verwendet, die mit diesem Netzwerknamen assoziiert war.

Wir empfehlen, den Parameter **Second Connection Attempt** nur in solchen Netzwerken auf **Enabled** zu setzen, die denen es häufiger zu Problemen mit DNS-Servern kommt und wo sich

die IP-Adressen der Maschinen selten ändern (ist z.B. der Fall bei festen IP-Adressen oder langen DHCP-Lease-Zeiten).

Diese Einstellung hat keinen Effekt auf Maschinen, die dem Management Server über eine IP-Adresse hinzugefügt wurden.

Offline Period Threshold (in Sekunden)

Beschreibung: Spezifiziert das maximale Intervall, in Sekunden, zwischen den erneuten Verbindungsversuchen zu einer registrierten Maschine, die offline zu sein scheint.

*Mögliche Werte:*Jede ganze Zahl zwischen **1800** und **2.147.483.647**

Standardwert: **1800**

Normalerweise verbindet sich der Management Server zu jeder registrierten Maschine nach einem bestimmten Zeitintervall (siehe **Period** und **Period-High Priority** zuvor in diesem Abschnitt). Wenn der Management Server entdeckt, dass die Maschine offline ist, verdoppelt er dieses Intervall; er behält die Verdopplung dieses Intervalls mit jedem Folgeversuch bei, bis der unter **Offline Period Threshold** spezifizierte Wert erreicht ist. Sobald die Maschine wieder online ist, wird das Zeitintervall erneut normal.

Dieser Ansatz hat das Ziel, die Ressourcen des Management Servers effizient zu nutzen und die Netzwerklast zu reduzieren.

Snapshot Storage

Spezifiziert den Ort und die Anfangsgröße des Storages für Snapshots – eine temporäre Datei, die beim Backup der Daten durch einen Snapshot benutzt wird. Die Datei wird gelöscht, sobald das Backup vollständig ist.

Mit den Standardeinstellungen wird der Snapshot-Storage im Ordner für temporäre Dateien des entsprechenden Agenten erstellt und belegt anfänglich 20 Prozent vom verfügbaren Speicherplatze des Volumes, das diesen Ordner enthält. Es wird mehr Platz verwendet, wenn das für den Snapshot erforderlich ist.

Sie können die Anfangsgröße für den Snapshot-Storage erhöhen – oder diesen auf ein anderes Volume verlegen – wenn Probleme mit dem Backup von Daten auftreten, die sich während des Backups umfangreich ändern.

Dieser Parameter wird bei Erstellung eines zentralen Backup-Plans verwendet. Änderungen an diesem Parameter haben keinen Einfluss auf bereits existierende zentrale Backup-Pläne.

Dieser Parameter hat die folgenden Einstellungen:

Pfad zum Snapshot-Ordner

Beschreibung: Spezifiziert das Verzeichnis, in dem der Snapshot-Storage platziert wird.

*Mögliche Werte:*Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: Leere Zeichenfolge

Eine leere Zeichenfolge entspricht dem Ordner '%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\MMS\Temp' (in Windows XP und Server 2003) oder '%PROGRAMDATA%\Acronis\BackupAndRecovery\MMS\Temp' (in Windows Vista und späteren Versionen von Windows).

Sie können einen lokalen Ordner auf einem beliebigen Volume angeben, einschließlich eines Volumes, das Sie sichern.

Pre-allocated storage size (in Megabyte)

Beschreibung: Spezifiziert die Anfangsgröße des Snapshot-Storages in Megabyte.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **2.147.483.647**

Standardwert: **0**

Lautet die Einstellung **0**, dann verwendet der Management Server die Einstellung **Pre-allocated storage size (in Prozent)**.

Die Anfangsgröße wird den verfügbaren Platz abzüglich 50 MB nicht überschreiten.

Pre-allocated storage size (in Prozent)

Diese Einstellung ist nur wirksam, wenn die Einstellung **Pre-allocated storage size (in Megabyte)** den Wert **0** hat.

Beschreibung: Spezifiziert die Anfangsgröße des Snapshot-Storages als Prozentwert des Festplattenplatzes, der zum Zeitpunkt des Backup-Starts zur Verfügung steht.

*Mögliche Werte:*Jede ganze Zahl zwischen **0** und **100**

Standardwert: **50**

Beträgt der Wert **0**, dann wird kein Snapshot-Storage erstellt.

Die Anfangsgröße wird den verfügbaren Platz abzüglich 50 MB nicht überschreiten.

Die Erstellung von Snapshots ist auch ohne Snapshot-Storage möglich.

Die Größe des Snapshot-Storages beeinflusst die Größe des Backups nicht.

Online Backup-Proxy

Spezifiziert die Proxy-Server-Einstellungen für Internetverbindungen zum Acronis Online Backup Storage.

Dieser Parameter hat die folgenden Einstellungen:

Proxy

Beschreibung: Spezifiziert, ob ein Proxy-Server verwendet werden soll.

Mögliche Werte: **Aktiviert** oder **Deaktiviert**

Standardwert: **Aktiviert**

Falls der Wert dieses Parameters **deaktiviert** ist, werden alle nachfolgenden Parameter ignoriert.

Adresse des Proxy-Servers

Beschreibung: Spezifiziert den Namen oder die IP-Adresse des Proxy-Servers

*Mögliche Werte:*Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: Leere Zeichenfolge

Port des Proxy-Servers

Beschreibung: Spezifiziert die Port-Nummer des Proxy-Servers

*Mögliche Werte:*Jede ganze Zahl zwischen 0 und 65535

Standardwert: **0**

Anmeldedaten für den Online Backup-Proxy

Verwenden Sie folgende zwei Parameter, falls der Proxy-Server zur Verbindung mit dem Acronis Online Backup Storage eine Authentifizierung erfordert.

Benutzername

Beschreibung: Spezifiziert den Benutzernamen zur Authentifizierung am Proxy-Server

*Mögliche Werte:*Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: Leere Zeichenfolge

Kennwort

Beschreibung: Spezifiziert das Kennwort zur Authentifizierung am Proxy-Server

*Mögliche Werte:*Jede Zeichenkette, 0 bis 32.765 Zeichen lang

Standardwert: Leere Zeichenfolge

Wichtig. Das Kennwort kann von jedem Benutzer eingesehen werden, der Zugriff auf das administrative Template hat – wie etwa ein Administrator der Maschine.

Programm zur Kundenzufriedenheit (CEP)

Beschreibung: Spezifiziert, ob der Management Server am Programm zur Kundenzufriedenheit (CEP) teilnimmt.

Mögliche Werte: **Aktiviert** (teilnehmen) oder **Deaktiviert** (nicht teilnehmen)

Standardwert: **Aktiviert**

15.5.1.5 Acronis Backup & Recovery 11.5 Management Console

Der nachfolgende Abschnitt erläutert die Parameter der Acronis Backup & Recovery 11.5 Management Console, die mit dem Acronis Administrative Template festgelegt werden können.

Auf Updates prüfen

Beschreibung: Spezifiziert, ob die automatische Prüfung auf Software-Updates jedes Mal durchgeführt wird, wenn Sie die Management Konsole starten.

Mögliche Werte: **Aktiviert** (Überprüfung durchführen) oder **Deaktiviert** (keine Überprüfung durchführen)

Standardwert: **Aktiviert**

Programm zur Kundenzufriedenheit (CEP)

Beschreibung: Spezifiziert, ob die Management Konsole am Programm zur Kundenzufriedenheit (CEP) teilnimmt.

Mögliche Werte: **Aktiviert** (teilnehmen) oder **Deaktiviert** (nicht teilnehmen)

Standardwert: **Aktiviert**

Smart Error Reporting

Beschreibung: Spezifiziert, ob bei einer von der Management Konsole angezeigten Fehlermeldung ein Link auf einen passenden Acronis Knowledge Base-Artikel eingeblendet wird.

Mögliche Werte: **Aktiviert** (einblenden) oder **Deaktiviert** (nicht einblenden)

Standardwert: **Aktiviert**

16 Online Backup

Dieser Abschnitt vermittelt Details zur Verwendung von Acronis Backup & Recovery Online. Dieser Service ermöglicht Online Backups zum Acronis Online Backup Storage.

Acronis Backup & Recovery Online ist möglicherweise in Ihrer Region nicht verfügbar. Zu weiteren Informationen klicken Sie hier: http://www.acronis.de/my/backup-recovery-online/

Um Backups zum Online Storage oder ein Recovery vom Online Storage einzurichten, folgen Sie den Schritten, die in den zugehörigen Abschnitten beschrieben sind:

Erstellung eines Backup-Plans (S. 58)

Einen zentralen Backup-Plan erstellen (S. 396)

Wiederherstellung von Daten (S. 146)

Der Hauptunterschied besteht darin, dass Sie den Online Storage als Backup-Ziel wählen.

Host-basierte Backups von virtuellen Maschinen sind mit der Virtual Edition von Acronis Backup & Recovery 11.5 möglich. Sie können alle durch den Agenten für ESX(i) oder Agenten für Hyper-V verwaltete Maschinen mit einem einzigen Abonnement für virtuelle Maschinen sichern.

16.1 Einführung in Acronis Backup & Recovery Online

Dieser Abschnitt enthält eine kurze Übersicht über Acronis Backup & Recovery Online und beantwortet Fragen, die möglicherweise während der Evaluierung oder Benutzung des Programms auftreten können.

16.1.1 Was ist Acronis Backup & Recovery Online?

Acronis Backup & Recovery Online ist ein Dienst, der Ihnen das Backup von Daten zum bzw. in den Acronis Online Backup Storage ermöglicht. Um diese Dienstleistung zu nutzen, müssen Sie ein Abonnement erwerben, welches den für Backups reservierten Speicherplatz (die Storage Quota) festlegt sowie den Zeitraum für die Nutzung des Online Services.

Beispiele für Abonnements:

- Ein Abonnement für mehrere Systeme vom Typ '1 TB/ 1 Jahr' bedeutet, dass Sie die Daten einer unbegrenzten Anzahl von physikalischen und/oder virtuellen Maschinen für den Zeitraum eines Jahres sichern können. Die Backups können nicht mehr als 1 Terabyte belegen.
- Ein Workstation-Abonnement vom Typ '250 GB/1 Jahr' bedeutet, dass Sie die entsprechenden Daten von einer Maschine, deren Betriebssystem kein Windows-Server-Betriebssystem ist, für ein ganzes Jahr sichern können. Die Backups können nicht mehr als 250 GB belegen.

16.1.2 Was für Daten können gesichert und wiederhergestellt werden?

Sie können Dateien, Volumes, Laufwerke oder die komplette physikalische Maschine so häufig wie gewünscht sichern. Anders als die meisten anderen Backup-Lösungen ermöglicht Acronis Backup & Recovery Online vom Online Storages aus auch eine Wiederherstellung auf fabrikneue Computer.

Einzelne Dateien können sowohl aus Laufwerk- wie auch Datei-basierten Backups wiederhergestellt werden.

Zu weiteren Informationen über das Backup virtueller Maschinen siehe „So können Sie virtuelle Maschinen zum Online Storage sichern (S. 461)“.

16.1.3 Wie lange werden Backups auf dem Online Storage aufbewahrt?

Ihr Backup verbleibt auf dem Online Storage, bis es von Ihnen gelöscht wird oder das Abonnement abläuft. Eine Datenwiederherstellung vom Online Storage ist bis zu 30 Tage nach Ablauf des Abonnements möglich.

Zur effektiven Nutzung des Online Storage-Speicherplatzes haben Sie die Möglichkeit, die Aufbewahrungsregel „**Lösche Backups älter als**“ einzustellen.

Beispiel

Für einen Datei-Server können Sie beispielsweise folgende Backup-Strategie verwenden.

Sichern Sie kritische Dateien zweimal täglich per Planung. Stellen Sie die Aufbewahrungsregel „**Lösche Backups älter als**“ auf 7 Tage ein. Das bedeutet, dass die Software nach jeder Sicherung überprüft, ob es Backups gibt, die älter als 7 Tage sind und diese dann automatisch löscht.

Führen Sie bei einem Server die Backups des System-Volumes manuell aus (wenn erforderlich). Beispielsweise nachdem Sie Betriebssystem-Updates aufgespielt haben. Löschen Sie nicht mehr benötigte Backups manuell.

16.1.4 Wie sicher sind die Daten?

Backups können mit Hilfe des kryptographischen Algorithmus 'Advanced Encryption Standard' (AES) und eines frei gewählten Kennworts verschlüsselt werden. Das gewährleistet, dass keine andere Person auf Ihre Daten zugreifen kann.

16.1.5 Wie kann ich virtuelle Maschinen zum Online Storage sichern?

Verwenden Sie eine oder beide der folgenden Methoden.

Installieren Sie die Acronis Software auf dem Virtualisierungshost

Dieser Ansatz ist praktisch, wenn das auf dem Host-Server installierte Virtualisierungsprodukt VMware ESX(i), Windows Server mit Hyper-V oder Microsoft Hyper-V Server ist.

Host-basierte Backups stehen nur für kommerzielle Lizenzen von VMware ESXi zur Verfügung. Sollte Ihr ESXi eine freie Lizenz verwenden, dann wählen Sie den weiter unten in diesem Abschnitt beschriebenen Ansatz.

Bei diesem Ansatz installieren Sie einen oder mehrere Acronis-Agenten auf den Virtualisierungshosts oder dedizierten Windows-Maschinen. Jeder Agent kann mehrere virtuelle Maschinen mit einem einzelnen Abonnement für virtuelle Maschinen per Backup sichern. Die erforderliche Anzahl an Abonnements muss daher der Anzahl der Agenten entsprechen. Alternativ können die Agenten auch ein Abonnement für mehrere Systeme verwenden, das mit anderen virtuellen und physikalischen Maschinen gemeinsam genutzt werden kann.

Sie können komplette virtuelle Maschinen oder einzelne Laufwerke bzw. Volumes sichern und wiederherstellen. Sie können zusätzlich einzelne Dateien und Ordner in das lokale Dateisystem des Agenten (nur bei Windows), zu einer Netzwerkfreigabe oder zu einem FTP- bzw. SFTP-Server wiederherstellen. Sie können Dateien direkt in das Dateisystem einer virtuellen Maschine wiederherstellen.

Die Installation der Software sowie die Durchführung von Backup- und Recovery-Aktionen sind im Dokument 'Backups von virtuellen Maschinen' für die Acronis Backup & Recovery 11.5 Virtual Edition beschrieben. Wenn Sie nur Acronis Backup & Recovery 11.5 Online Backup installieren, müssen Sie während der Installation keinen Lizenzschlüssel eingeben.

Da ESX(i)-Maschinen automatisch zwischen den Agenten verteilt werden können, müssen Sie die Maschinen manuell an ihre Agenten anbinden, damit die Maschinen immer dasselbe Abonnement verwenden.

Installieren Sie die Acronis Software auf dem Gastsystem

Dieser Ansatz gilt nur für virtuelle Maschinen, die unter Windows laufen.

Dieser Ansatz ist für folgende Situationen geeignet:

- die Maschine wird nicht auf einem Virtualisierungsserver gehostet
- das auf dem Host-Server installierte Virtualisierungsprodukt ist *nicht* VMware ESX(i), Windows Server mit Hyper-V oder Microsoft Hyper-V Server
- Sie möchten ein unabhängiges Laufwerk oder ein RDM-Laufwerk (über den physikalischen Kompatibilitätsmodus angebunden) auf einer laufenden ESX(i)-Maschine sichern
- Sie möchte ein Pass-Through-Laufwerk (Durchleitungslaufwerk) einer virtuellen Hyper-V-Maschine sichern
- Sie möchten Befehle vor/nach dem Backup bzw. vor/nach der Datenerfassung auf der virtuellen Maschine verwenden
- Sie möchten einzelne Dateien und Ordner der virtuellen Maschine sichern
- Sie möchten Dateien direkt in das Dateisystem der virtuellen Maschine wiederherstellen.

Die virtuelle Maschine wird wie eine physikalische Maschine behandelt. Falls Sie kein Abonnement für mehrere Systeme haben, benötigen Sie für diese Maschine ein separates Server- oder Workstation-Abonnement.

Die Installation der Software sowie die Durchführung von Backup- und Recovery-Aktionen entsprechen denen auf einer physikalischen Maschine.

16.1.6 Unterstützte Betriebssysteme und Virtualisierungsprodukte

Von Acronis Backup & Recovery Online unterstützte Server-Betriebssysteme:

Windows 2000 SP4 – alle Editionen, mit Ausnahme der Datacenter und Professional Editionen

Windows Server 2003/2003 R2 – Standard und Enterprise Editionen (x86, x64)

Windows Small Business Server 2003/2003 R2

Windows Server 2008 – Standard, Enterprise, Datacenter und Web Editionen (x86, x64)

Windows Small Business Server 2008

Windows Server 2008 R2 – Standard, Enterprise, Datacenter, Foundation und Web Editionen

Windows MultiPoint Server 2010/2011

Windows Small Business Server 2011 – alle Editionen

Windows Server 2012/2012 R2 – alle Editionen

Windows Storage Server 2003/2008/2008 R2/2012

Von Acronis Backup & Recovery Online unterstützte Workstation-Betriebssysteme:

Windows 2000 Professional SP4

Windows XP Professional SP2+ (x86, x64)

Windows Vista – alle Editionen mit Ausnahme von Vista Home Basic und Vista Home Premium (x86, x64)

Windows 7 – alle Editionen mit Ausnahme der Starter und Home Editionen (x86, x64)

Windows 8/8.1 – alle Editionen mit Ausnahme der Windows RT-Editionen (x86, x64)

Von Acronis Backup & Recovery Online unterstützte Virtualisierungsprodukte (Host-basiertes Backup von virtuellen Maschinen):

VMware ESX Infrastructure 3.5 Update 2+

VMware ESX(i) 4.0, 4.1, 5.0, 5.1 und 5.5

(Host-basierte Backups stehen nur für kommerzielle Lizenzen von VMware ESXi zur Verfügung).

Windows Server 2008 (x64) mit Hyper-V

Windows Server 2008 R2 mit Hyper-V

Microsoft Hyper-V Server 2008/2008 R2

Windows Server 2012/2012 R2 mit Hyper-V

Microsoft Hyper-V Server 2012/2012 R2

16.1.7 FAQ zu Backup und Recovery

Dieser Abschnitt beantwortet typische Fragen zu Backup- und Recovery-Aktionen

16.1.7.1 Welche Backup-Methoden sind verfügbar?

Vollständige und inkrementelle Backup-Methoden stehen in mehreren Backup-Schemata zur Verfügung. Die erste Task-Ausführung produziert unabhängig vom jeweiligen Backup-Schema ein Voll-Backup; nachfolgende Task-Ausführungen erstellen dann inkrementelle Backups. Folgende Backup-Schemata stehen zur Verfügung:

- **Jetzt ausführen** (sofortiger Start) oder **Manueller Start** (verzögerter Start). Sie können den Task erneut manuell ausführen.
- **Einfach** (Start nach Planung). Sie können mit diesem Backup-Schema eine Aufbewahrungsregel zur automatischen Löschung alter Backups einstellen.
- **GVS (Großvater-Vater-Sohn)** (Start nach Planung). Sie spezifizieren, welche der täglichen Backups als wöchentliche und monatliche Backups betrachtet werden sollen. Sie können separate Aufbewahrungsregeln für tägliche, wöchentliche und monatliche Backups einrichten.
- **Türme von Hanoi** (Start nach Planung). Sie legen die Anzahl der Level fest. Dies ist die Anzahl der zu einem Zeitpunkt gespeicherten Backups. Überschüssige Backups werden so gelöscht, dass mehr Recovery-Punkte für jüngere und weniger für ältere Zeitpunkte übrigbleiben.
- Ein weiteres, nur für den Online Storage verfügbares Backup-Schema ist **Initial Seeding**. Mit diesem Schema startet das Backup sofort zu einem lokalen Zielspeicherort und verwendet die Voll-Backup-Methode. Um dieses Schema zu verwenden, benötigen Sie eine 'Initial Seeding (S. 79)'-Lizenz.

16.1.7.2 Welche Recovery-Methoden sind verfügbar?

Es gibt zwei Methoden, wie Sie Ihre Daten vom Acronis Online Backup Storage wiederherstellen können:

- Die Wiederherstellung von von Laufwerken oder Dateien unter Verwendung der Benutzeroberfläche oder Befehlszeilenschnittstelle von Acronis Backup & Recovery 11.5. Mit dieser Methode können Sie im weiten Rahmen auf die Acronis Backup & Recovery 11.5-Funktionalität zurückgreifen.
- Die Wiederherstellung von Dateien (S. 480) aus dateibasieren Backups unter Verwendung eines Webbrowsers. Zur Nutzung dieser Option benötigen Sie nur eine Maschine mit Internetzugang.

16.1.7.3 Ist der Online Storage auch von Acronis Bootable Media aus verfügbar?

Wiederherstellungen vom Acronis Online Backup Storage sind möglich, Backups zum Online Storage dagegen nicht.

16.1.7.4 Kann Acronis Universal Restore verwendet werden, wenn eine Systemwiederherstellung vom Online Storage aus erfolgt?

Ja. Acronis Universal Restore ist immer verfügbar, wenn Sie ein System aus dem Online Storage wiederherstellen. Der Einsatz von Acronis Universal Restore bei Wiederherstellungen aus anderen Storage-Typen erfordert jedoch eine separate Lizenz.

16.1.7.5 Was passiert, wenn während einer Online Backup- oder Recovery-Aktion die Netzwerkverbindung verloren geht?

Die Software wird alle 30 Sekunden versuchen, den Online Storage zu erreichen. Die Versuche werden aufgegeben, wenn die Verbindung entweder wieder aufgenommen wird – oder eine bestimmte Anzahl an Versuche durchgeführt wurde (je nachdem, was zuerst eintritt). Die Standardanzahl an Versuchen ist 300 bei Backups und 30 bei Wiederherstellungen.

Sie können die Zahl der Versuche und die Zeitspanne zwischen den Versuchen unter **Fehlerbehandlung** mit der Option **Bei Fehler erneut versuchen** ändern. Jeder Backup-Plan oder Recovery-Task enthält diese Option.

16.1.7.6 Was passiert, wenn Ihnen der Speicherplatz ausgeht?

Wenn die Backups einer Maschine den per Abonnement erlaubten Speicherplatz zu überschreiten drohen, erhalten Sie eine Alarmmeldung per E-Mail. Sie können diese Alarmmeldung auch auf der Webseite zur Kontoverwaltung sehen (neben der Maschine). Das bedeutet, dass Sie für zukünftige Backups Speicherplatz freimachen müssen. Oder Sie könnten erwägen, die Storage-Quota zu erhöhen (S. 474). Sie können auch eine Aufbewahrungsregel (S. 461) einstellen oder bearbeiten, damit zukünftig kein Überlauf mehr auftritt. Sobald der belegte Speicherplatz das Limit erreicht, verweigern die Backups ihre Ausführung.

16.1.7.7 Wofür ist der Bereinigungstask gedacht?

Jeder Backup-Plan mit gesetzter Bereinigungsregel enthält zusätzlich zum Backup-Task auch einen Bereinigungstask. Der Bereinigungstask überprüft das auf Basis des Backup-Plans erstellte Archiv nach Backups, die ihre 'Lebensdauer' überschritten haben. Wenn solche Backups gefunden werden,

bewirkt der Task, dass der Online Storage diese löscht. Da die Löschung auf Seiten des Online Storage durchgeführt wird, werden keine CPU-Ressourcen von Ihrer Maschine beansprucht.

Der Bereinigungstask läuft nach jedem Online Backup, auch wenn das Backup selbst fehlgeschlagen ist. Zudem wird auch immer das letzte erfolgreiche Backup bewahrt. Weitere Informationen über die Aufbewahrungsregel finden Sie unter „Wie lange werden Backups auf dem Online Storage aufbewahrt? (S. 461)“.

Es ist normalerweise nicht notwendig, den Bereinigungstask manuell zu starten oder zu stoppen. Sie können dies jedoch in der Ansicht **Backup-Pläne und Tasks** tun.

16.1.7.8 Wie bewirken Sie, dass eine wiederhergestellte Maschine ihr Abonnement erkennt?

Wenn Sie eine physikalische Maschine aus einem Backup wiederherstellen, wird auch ein neuer 'Machine Identifier' erstellt. Daher kann die Maschine keine Backups zu dem Abonnement durchführen, das sie vor der Recovery-Aktion verwendet hat.

Um die Maschine zum selben Abonnement zu sichern, müssen Sie dieses der Maschine erneut zuweisen (S. 478). Wenn Sie dies tun, können die nächsten Backups der Maschine wieder inkrementell sein. Wenn Sie der Maschine ein neues Abonnement zuweisen, muss die Software ein neues Voll-Backup durchführen.

16.1.8 FAQ zu Initial Seeding

Dieser Abschnitt erklärt, was Initial Seeding ist, warum es für Sie vorteilhaft ist und zudem einige Details zu seiner Verwendung.

16.1.8.1 Was ist Initial Seeding?

Initial Seeding ist ein Extra-Service, bei dem Sie das initiale Voll-Backup lokal ausführen und dieses dann auf einer Festplatte (oder einem ähnlichen Laufwerk) an Acronis senden.

Acronis lädt das Backup dann zum Online Storage hoch. Danach können Sie dieses Voll-Backup – manuell oder nach Zeitplan – mit nachfolgenden inkrementellen Backups erweitern.

Das Laufwerk erhalten Sie zurück, aber es ist nicht möglich, davon ein Recovery durchzuführen. Ein Recovery ist von einem lokal angeschlossenen Gerät jedoch mit der Option 'Large Scale Recovery (S. 471)' möglich.

16.1.8.2 Wann ist Initial Seeding sinnvoll?

Dieser Dienst hilft Ihnen, beim initialen Voll-Backup Zeit und Netzwerkverkehr zu sparen. Das ist nützlich, wenn Sie sehr große Datenmengen oder komplette Maschinen zum Online Storage sichern.

16.1.8.3 Ist Initial Seeding ein kostenpflichtiger Dienst?

Ja, Sie benötigen eine 'Initial Seeding'-Lizenz für jede Maschine.

16.1.8.4 Welche Laufwerkstypen können für Initial Seeding verwendet werden?

Acronis akzeptiert Festplatten (und ähnliche Laufwerke) mit folgenden Schnittstellentypen: IDE, ATA, SATA sowie per USB angeschlossene Laufwerke. SCSI-Laufwerke werden nicht akzeptiert.

Sie können das Backup direkt auf das Gerät erstellen lassen – oder auf einen lokalen Ordner oder Netzwerkordner speichern und das Backup anschließend auf das Gerät kopieren. Sorgen Sie dafür, dass das Gerät nur ein Volume hat und das Dateisystem NTFS oder FAT32 verwendet.

16.1.8.5 Kann mehr als ein Backup pro einzelner 'Initial Seeding'-Lizenz übermittelt werden?

Nein. Eine 'Initial Seeding'-Lizenz erlaubt Ihnen nur die Erstellung jeweils eines Backups auf der Maschine.

Sollten Sie jedoch einen Fehler gemacht haben oder aus irgendeinem Grund ein anderes Backup erstellen wollen, dann können Sie den 'Initial Seeding'-Auftrag auch abbrechen. Die Lizenz wird daraufhin wieder verfügbar.

16.1.8.6 Können Backups mehrerer Maschinen auf einem Laufwerk übermittelt werden?

Ja. Sie benötigen aber dennoch je eine Lizenz pro Maschine.

16.1.8.7 Wie kann eine 'Initial Seeding'-Lizenz erworben werden?

Sie können eine 'Initial Seeding'-Lizenz von einem Acronis-Partner oder im Acronis Online Store kaufen. Verwenden Sie den Link http://www.acronis.de/my/backup-recovery-online/#buy, um einen Partner zu finden oder einen Online-Kauf durchzuführen.

Nachdem Sie eine Lizenz von einem Acronis-Partner erworben haben, erhalten Sie eine Bestätigungs-E-Mail mit einem Registrierungscode. Klicken Sie auf derselben Webseite auf **Neuen Registrierungscode eingeben** und registrieren Sie die Lizenz. Die Lizenz wird dann über die Registerlasche **Initial Seeding / Recovery** zur Verfügung gestellt.

Eine über den Acronis Online Store erworbene Lizenz wird unmittelbar nach Abschluss des Zahlvorgangs verfügbar.

16.1.8.8 Wie führe ich Initial Seeding aus?

1. Stellen Sie sicher, dass Sie ein Acronis Backup & Recovery Online-Abonnement auf der Maschine aktiviert haben, für die Sie die Initial Seeding-Prodezur durchführen wollen (überspringen Sie diesen Schritt, falls Sie ein Abonnement für mehrere Systeme haben).
2. Falls Sie gerade ein Testabonnement verwenden, sollten Sie sicherstellen, dass Sie auch über ein bezahltes Abonnement verfügen und es der Maschine zugewiesen haben. Verwenden Sie den Initial Seeding Service nicht, wenn Sie kein bezahltes Abonnement haben.
3. Entscheiden Sie sich für das Medium (S. 466), welches Sie für den Versand verwenden wollen.
4. Schließen Sie das Medium bzw. Laufwerk an die Maschine an, die Sie per Backup sichern wollen. Alternativ können Sie das Backup auch zu einem lokalen Ordner oder einer Netzwerkfreigabe sichern – und es anschließend dann auf das Medium kopieren/verschieben.

5. Starten Sie Acronis Backup & Recovery 11.5, klicken Sie auf **Backup-Plan erstellen** und erstellen Sie auf dieser Maschine einen Backup-Plan:
   - Wählen Sie bei **Backup-Quelle** die Laufwerke/Volumes oder Dateien/Ordner, die Sie sichern wollen.
   - Spezifizieren Sie den **Online Backup Storage** als **Backup-Ziel**.
   - Wählen Sie bei **Backup-Schema** die Einstellung **Initial Seeding**. Spezifizieren Sie das besprochene Medium als Backup-Ziel.
   - [Optional, aber dringend empfohlen] Aktivieren Sie unter **Backup-Optionen** –> **Schutz des Archivs** eine Verschlüsselung für das Backup.

   Das Backup startet unmittelbar, sobald Sie abschließend auf **OK** klicken.
6. [Optional] Wenn Sie Backups von einer anderen Maschine hinzufügen wollen, dann schließen Sie das Medium an diese Maschine an und wiederholen Sie die entsprechenden Schritte. Sie benötigen für jede Maschine, die Sie per Backup sichern wollen, eine separate Initial Seeding-Lizenz.
7. Verpacken (S. 467) Sie das Medium zusammen mit einem frankierten Rücksendeetikett und senden Sie es über den herkömmlichen Postweg an Acronis. Sie finden die Adresse auf der Webseite zur Kontoverwaltung unter **Initial Seeding / Recovery** –> **Laufende Aufträge** –> **Initial Seeding-Aufträge** –> **Datacenter-Adresse**.
8. Kennzeichnen Sie auf derselben Webseite den Auftrag als 'Versendet' und verfolgen (S. 469) Sie den Auftragsstatus.
9. Sobald Sie sehen, dass das Backup auf den Online Storage hochgeladen wurde, können Sie den Backup-Plan so bearbeiten, dass inkrementelle Backups erstellt werden.
   - Wählen Sie bei **Backup-Schema** das gewünschte Backup-Schema und spezifizieren Sie dessen Einstellungen.
   - Klicken Sie auf **Speichern**.

   Ihr Backup-Plan wird bei manuellem oder geplantem Start dem anfänglichen, auf dem Online Storage gespeicherten Backup weitere inkrementelle Backups hinzufügen.

16.1.8.9 Wie verpacken Sie ein Laufwerk zur Versendung richtig?

Es ist sehr wichtig, dass Sie Ihre Festplatte (oder ein ähnliches Laufwerk) sorgfältig für den Versand verpacken. Durch eine gute Verpackung schützen Sie Ihr Laufwerk vor Transportschäden.

Laufwerkstypen

Acronis akzeptiert Festplatten (und ähnliche Laufwerke) mit folgenden Schnittstellentypen: Per IDE, ATA, SATA sowie USB anschließbare Laufwerke.

SCSI-Laufwerke werden nicht akzeptiert.

Verpackung

Verwenden Sie – sofern möglich/verfügbar – die Originalverpackung des Laufwerks. Anderenfalls können Sie geeignetes Verpackungsmaterial auch bei entsprechenden Poststationen oder ähnlichen Geschäften erhalten. Sie sollten dem Laufwerk außerdem alle benötigten Kabel und Adapter beilegen. Acronis kann Ihre 'Initial Seeding'-Anforderung nicht bearbeiten, falls der Sendung keine passenden Kabel beiliegen.

Nachfolgend finden Sie Hinweise zur geeigneten Verpackung Ihres Laufwerks.

Schritt 1

Entfernen Sie Ihr Laufwerk vorsichtig von der entsprechenden Maschine.



Schritt 2

Stecken Sie das Laufwerk in eine Antistatikhülle, um es vor elektrostatischen Entladungen zu schützen. Falls Sie keine Antistatikhülle zur Verfügung haben, können Sie das Laufwerk alternativ auch mit Alufolie umwickeln.

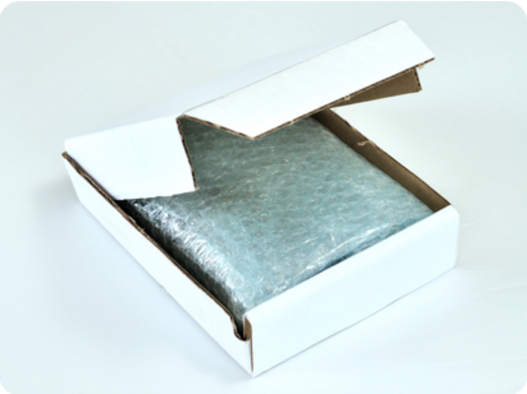


Schritt 3

Verwenden Sie eine stabile Box, die mindestens doppelt so groß wie das Laufwerk ist. Wickeln Sie das Laufwerk über alle 6 Seiten mit einer Luftpolsterfolie so ein, dass es genau in die Box passt und sich in dieser nicht bewegen kann.

*Verwenden Sie **keine** Styropor-**Chips** zur Verpackung, da diese nicht genügend Schutz bieten.*
*Versenden Sie das Laufwerk **nicht** einfach in einer herkömmlichen **gepolsterten Versandtasche**.*





Schritt 4

Wählen Sie den von Ihnen gewünschten Paketdienst für den Versand. Erstellen bzw. bedrucken Sie (z.B. über eine entsprechende Website des Paketdienstes) zwei bereits frankierte Versandetiketten:

1. Das **Versandetikett zur Hinsendung** Ihres Laufwerks. Dieses Etikett gehört auf die Oberseite der Box. Sie müssen das Paket dann an ein Acronis Datacenter versenden. Die Adresse des entsprechenden Datacenters finden Sie auf der Webseite zur Kontenverwaltung innerhalb der Registerlasche **Initial Seeding/Recovery** (indem Sie auf den Befehl **Datacenter-Adresse** klicken).

   Falls Sie möglichst schnell mit der Erstellung inkrementeller Backups beginnen wollen, sollten Sie erwägen, einen Express- bzw. Nachtversanddienst zu verwenden. Sobald die Daten beim Datacenter eingetroffen sind, stehen Sie üblicherweise am darauf folgenden Arbeitstag zur Verfügung.
2. Das **Versandetikett zur Rücksendung** Ihres Laufwerks. Legen Sie dieses Etikett in die Box zum Laufwerk. Zur Rücksendung wird dieselbe Verpackung verwendet (sofern sie nicht beschädigt wurde). Wenn Sie Ihrer Sendung kein frankiertes Etikett beilegen, wird Ihr Laufwerk **sicher entsorgt**.

   Sie können zur Rücksendung Ihres Laufwerks eine kostengünstige Methode bzw. einen Paketdienst Ihrer Wahl verwenden.



Schritt 5

Versiegeln Sie die Box sicher mit einem stabilen Klebeband. Kleben Sie dann das **Versandetikett zur Hinsendung** Ihres Laufwerks auf die Oberseite der Box und achten Sie darauf, dass das Etikett nicht über eine der Kanten geklebt ist.



16.1.8.10 Wie kann der Auftragsstatus für Initial Seeding verfolgt werden?

Auf der Acronis-Website zeigt die Registerlasche **Initial Seeding / Recovery** den Status aller Aufträge. Sie erhalten zusätzlich eine E-Mail-Benachrichtigung über wichtige Ereignisse.

- **Verfügbar** – Die Lizenz kann für jede Maschine verwendet werden.
- **Ein Auftrag wurde erstellt** – Das Backup ist bereit für den Start und die Lizenz kann weder für dieselbe, noch eine andere Maschine erneut verwendet werden. Sie können von hier an den Auftrag aber noch abbrechen, wenn etwas falsch läuft. Dadurch wird die Lizenz an den Pool verfügbarer Lizenzen zurückgegeben.
- **Ein Voll-Backup wurde gestartet** – Dieser Zustand wird eingestellt, wenn das erste Backup ausgeführt wird. Ab diesem Moment beginnt die Laufzeit des Vertrags.
- **Ein Voll-Backup wurde erfolgreich abgeschlossen** – Das Backup wurde fertig gestellt und der Auftrag ist bereit zur Versendung. Sie können das Medium jetzt verschicken:

  Schritt 1. Verpacken Sie das Medium gemäß der Anleitung für Verpackung und Versand des Laufwerks (S. 467), um Transportschäden zu vermeiden. Falls Sie wollen, dass das Medium nach dem Upload der Daten an Sie zurückgeschickt wird, legen Sie der Verpackung neben dem Laufwerk auch ein vorbereitetes, ausreichend frankiertes Rücksendeetikett bei.

  Schritt 2. Verschicken Sie das Laufwerk mit dem von Ihnen gewünschten Paketdienst zum Acronis Datacenter.

  Schritt 3. Teilen Sie uns den Versand des Pakets mit, indem Sie Ihren Auftrag als „Versendet“ kennzeichnen.

  Sie erhalten eine Benachrichtigung, sobald Acronis den Auftrag erhalten hat und sobald der Auftrag abgeschlossen wurde. Sofern erforderlich, werden Sie von Acronis während der Auftragsbearbeitung kontaktiert.
- [Gelegentlich] **Fehler bei Backup-Erstellung** – Während der Sicherung ist ein Fehler aufgetreten. Überprüfen Sie die Parameter des Backup-Plans und versuchen Sie es dann erneut.
- **Das Medium wurde versendet** – Dieser Status wird eingestellt, nachdem Sie den Auftrag mit „Versendet“ gekennzeichnet haben.
- **Das Medium wurde von Acronis erhalten** – Acronis hat mit der Bearbeitung Ihres Auftrages begonnen. Von diesem Punkt an können Sie den Auftrag nicht mehr abbrechen. Die Erstellung eines neuen 'Initial Seeding'-Backups erfordert eine neue 'Initial Seeding'-Lizenz.
- **Der Upload der Daten wurde gestartet** – Das Upload der Daten zum Acronis Online Backup Storage hat begonnen.
- **Der Upload der Daten wurde abgeschlossen** – Das anfängliche Voll-Backup wurde erfolgreich auf den Online Storage hochgeladen. Sie können nun inkrementelle Online Backups durchführen.
- **Der Auftrag wurde ausgeführt. Das Medium wurde zurückgeschickt** (oder: **Rücksendung des Mediums wurde nicht angefordert**) – Das Medium wurde zurückgeschickt (Paketdienst und Sendeverfolgungsnummer sind angegeben). Falls dem Medium kein frankiertes Versandetikett beigelegt wurde, wird das Medium entsorgt.
- [Gelegentlich] **Auftrag ist in Wartestellung** – Ihr Auftrag wurde wegen technischer Schwierigkeiten bei der Auftragsbearbeitung unterbrochen. Acronis arbeitet an einer Lösung der Probleme.
- [Gelegentlich] **Der Auftrag wurde abgebrochen** – Der Auftrag wurde noch vor Versendung des Mediums abgebrochen, dessen Rücksendung ist daher nicht erforderlich.
- [Gelegentlich] **Der Auftrag wurde abgebrochen. Das Medium wurde zurückgeschickt** (oder: **Rücksendung des Mediums wurde nicht angefordert**) – Der Auftrag wurde abgebrochen, während das Medium im Datacenter war. Das Medium wurde zurückgeschickt (Paketdienst und Sendeverfolgungsnummer sind angegeben). Falls dem Medium kein frankiertes Versandetikett beigelegt wurde, wird das Medium entsorgt.

16.1.9 FAQ zu Large Scale Recovery

Dieser Abschnitt erklärt, was Large Scale Recovery ist, warum es für Sie vorteilhaft ist und zudem einige Details zu seiner Verwendung.

16.1.9.1 Was ist Large Scale Recovery?

Large Scale Recovery ist ein Extra-Service, mit dem Sie eine Kopie der Backups erhalten, welche sich im Online Storage befinden. Anschließend können Sie die Daten aus dieser Kopie wiederherstellen.

Sobald Sie ein Large Scale Recovery für eine bestimmte Maschine ordern, sendet Acronis Ihnen ein USB-Laufwerk mit allen Backups, die Sie von dieser Maschine erstellt haben. Sie können die Daten direkt vom Laufwerk wiederherstellen oder die Backups zu einem lokalen oder Netzwerkordner kopieren.

16.1.9.2 Wann ist Large Scale Recovery sinnvoll?

Der Dienst hilft Zeit und Netzwerkverkehr zu sparen, beispielsweise im Desasterfall, bei Wiederherstellung großer Datenmengen oder kompletter Maschinen. Eine Wiederherstellung von Daten im Bereich vieler Hundert Gigabytes über das Internet kann Tage dauern. Dieser Prozess ermöglicht Ihnen eine schnellere Wiederherstellung.

16.1.9.3 Muss Initial Seeding zur Nutzung von Large Scale Recovery ausgeführt werden?

Nein, diese Dienstleistungen sind voneinander unabhängig.

16.1.9.4 Ist Large Scale Recovery kostenpflichtig?

Ja, Sie benötigen je eine Lizenz für Large Scale Recovery pro Maschine. Durch diese Lizenz wird Ihnen bei Bedarf ein Laufwerk zugeschickt, das alle aktuell verfügbaren Backups dieser Maschine enthält. Um auch zukünftige Backups zu erhalten, benötigen Sie eine neue 'Large Scale Recovery'-Lizenz.

16.1.9.5 Kann ein Large Scale Recovery auf einer anderen Maschine erfolgen?

Ja. Sie können Ihre Daten beliebig oft auf jeder gewünschten Maschine wiederherstellen. Acronis Universal Restore ist bereits integriert, so dass Sie ein Betriebssystem auch auf abweichender Hardware wiederherstellen können.

16.1.9.6 Können Backups mehrerer Maschinen gemeinsam auf einem Laufwerk zurückerhalten werden?

Nein. Es ist ein separates Laufwerk für jede Maschine erforderlich.

16.1.9.7 Wie kann eine Lizenz für Large Scale Recovery erworben werden?

Sie können eine 'Large Scale Recovery'-Lizenz von einem Acronis-Partner oder im Acronis Online Store kaufen. Verwenden Sie den Link www.acronis.de/my/backup-recovery-online/#buy, um einen Partner zu finden oder einen Online-Kauf durchzuführen.

Nachdem Sie eine Lizenz von einem Acronis-Partner erworben haben, erhalten Sie eine Bestätigungs-E-Mail mit einem Registrierungscode. Klicken Sie auf derselben Webseite auf **Neuen Registrierungscode eingeben** und registrieren Sie die Lizenz. Die Lizenz wird dann über die Registerlasche **Initial Seeding / Recovery** zur Verfügung gestellt.

Eine über den Acronis Online Store erworbene Lizenz wird unmittelbar nach Abschluss des Zahlvorgangs verfügbar.

16.1.9.8 Wie kann der Auftragsstatus für Large Scale Recovery verfolgt werden?

Auf der Acronis-Website zeigt die Registerlasche **Initial Seeding / Recovery** den Status aller Aufträge. Sie erhalten zusätzlich eine E-Mail-Benachrichtigung über wichtige Ereignisse.

- **Verfügbar** – Die Lizenz kann für eine beliebige Maschine verwendet werden.
- **Ein Auftrag wurde erstellt** – Dieser Status ist nach Auftragsabschluss für Large Scale Recovery eingestellt. Diese Lizenz kann nicht mehr für eine andere Maschine verwendet werden. Sie können von diesem Punkt an den Auftrag auch abbrechen, wenn etwas falsch läuft. Dadurch wird die Lizenz an den Pool verfügbarer Lizenzen zurückgegeben.
- **Der Auftrag wird bearbeitet** – Das Data Center hat mit der Auftragsbearbeitung begonnen.
- **Schreibe Daten** – Ihre Backups werden gerade auf das Medium geschrieben. Von diesem Punkt an können Sie den Auftrag nicht mehr abbrechen.
- **Schreiben der Daten wurde abgeschlossen** – Ihre Backups wurden erfolgreich auf das Medium geschrieben.
- **Bereit, das Medium zu versenden** – Ihr Auftrag wurde bearbeitet und das Medium wird in Kürze verschickt.
- **Der Auftrag wurde ausgeführt. Das Medium wurde versendet** – Das Medium wurde an Sie verschickt (Transportunternehmen und Sendeverfolgungsnummer sind angegeben).
- [Gelegentlich] **Auftrag ist in Wartestellung** – Ihr Auftrag wurde wegen technischer Schwierigkeiten bei der Bearbeitung des Auftrages pausiert. Acronis arbeitet an einer Lösung der Probleme.
- [Gelegentlich] **Der Auftrag wurde abgebrochen** – Der Auftrag wurde abgebrochen.
- [Gelegentlich] **Adresse ist nicht zustellbar** – Acronis kann das Laufwerk nicht verschicken. Klicken Sie auf der gleichen Webseite auf **Meine Lieferadresse ändern** und spezifizieren Sie die richtige Adresse für den Auftrag.
- [Gelegentlich] **Adresse wurde aktualisiert** – Dieser Status wird eingestellt, nachdem Sie die Zustelladresse auf der Acronis-Website geändert haben.

16.1.9.9 Wie wird Large Scale Recovery ausgeführt?

Der Recovery-Vorgang ist identisch zu anderen Wiederherstellungen vom Online Storage. Sie spezifizieren lediglich den Pfad zum Speicherort Ihrer Backups. Weitere, detaillierte Informationen zu Recovery-Aktionen finden Sie in der kontextabhängigen Hilfe.

16.1.10 FAQ zum Abonnement-Lebenszyklus

Dieser Abschnitt erläutert den Lebenszyklus eines Abonnement und die Aktionen mit Abonnements, die Sie auf der Webseite zur Kontonverwaltung ausführen können.

16.1.10.1 Wie kann auf die Webseite zur Kontoverwaltung zugegriffen werden?

So gelangen Sie über die Acronis-Website auf die entsprechende Webseite:

1. Wählen Sie **Mein Konto**.
2. Melden Sie sich mit Ihrem Konto an (oder erstellen Sie ein Konto, falls Sie noch nicht registriert sind).
3. Navigieren Sie zu **Online Backup** –> **für Unternehmen**.

So gelangen Sie über Acronis Backup & Recovery 11.5 auf die entsprechende Webseite:

1. Klicken Sie im Menü **Aktionen** auf **Backup jetzt** oder **Backup-Plan erstellen**.
2. Klicken Sie auf **Speicherort** und dann auf **Abonnements erwerben oder verwalten**.
3. Melden Sie sich mit Ihrem Konto an (oder erstellen Sie ein Konto, falls Sie noch nicht registriert sind).

16.1.10.2 Wo sind erworbene Abonnements zu finden?

Wenn Sie Abonnements von einem Acronis-Partner erworben haben, sollten Sie eine Bestätigungs-E-Mail mit den Registrierungscodes für jedes Abonnement erhalten haben. Erstellen Sie – falls noch nicht vorhanden – ein Konto auf der Acronis-Website und melden Sie sich an. Navigieren Sie zu **Online Backup** –> **Für Unternehmen**. Das ist die *Webseite zur Kontoverwaltung*. Klicken Sie auf **Neuen Registrierungscode eingeben** und registrieren Sie die Lizenz. Diese Abonnements erscheinen in der Liste verfügbarer Abonnements in der Registerlasche **Abonnements verwalten**.

Wenn Sie Abonnements online über die Acronis-Website erworben haben, können Sie diese unverzüglich auf der Webseite zur Kontoverwaltung finden. Neu erhaltene Abonnements sind in der Registerlasche **Abonnements verwalten** aufgelistet.

16.1.10.3 Wann beginnt ein Abonnement?

Bei Abonnements **für mehrere Systeme** beginnt der Abonnementzeitraum mit dem Tag des Erwerbs.

Bei Abonnements **pro System** beginnt der Abonnementzeitraum, sobald ein Abonnement auf der Maschine aktiviert wurde.

16.1.10.4 Was passiert bei Ablauf eines Abonnements?

Einen Monat vor Ablaufdatum des Abonnements erhalten Sie eine Alarmmeldung per E-Mail. Sie können diese Alarmmeldung auch auf der Webseite zur Kontoverwaltung sehen (neben der Maschine). Das bedeutet, dass Sie das Abonnement erneuern (S. 473) müssen, um mit den Backups der Maschine fortfahren zu können.

Falls Sie das Abonnement nicht erneuern, können Sie noch weitere fünf Tage nach Ablaufdatum zum Online Storage sichern. Sie können Daten aus dem Online Storage noch bis zu 30 Tage nach Ablaufdatum wiederherstellen.

16.1.10.5 Wie wird ein Abonnement erneuert?

Erwerben Sie ein anderes Abonnement und spezifizieren Sie dieses als nächstes Abonnement für die Maschine. Das neue Abonnement wird aktiviert, sobald das aktuelle Abonnement endet.

Ein abgelaufenes Abonnement kann innerhalb von fünf Tagen nach Ablauf erneuert werden. In solchen Fällen wird das neue Abonnement unverzüglich aktiviert.

Ein einzelnes Abonnement erneuern

So erneuern Sie ein Abonnement

1. Gehen Sie zur Webseite der Kontoverwaltung.
2. Sorgen Sie dafür, dass Sie über ein Abonnement des gleichen Typs und mit der gleichen oder einer größeren Storage Quota verfügen.

   Beispiel: Um ein 'Acronis Backup & Recovery Online Workstation 250GB'-Abonnement zu erneuern, benötigen Sie entweder ein 'Acronis Backup & Recovery Online Workstation 250GB'-Abonnement oder ein 'Acronis Backup & Recovery Online Workstation 500GB'-Abonnement.
3. Wählen Sie die Maschine, deren Abonnement Sie erneuern wollen und klicken Sie dann auf **Erneuern**.

Das Abonnement erscheint für die gewählte Maschine in der Spalte **Nächstes Abonnement**.

Mehrere aktivierte Abonnements auf einmal erneuern

Diese Aktion ist möglich, wenn die Anzahl der neuen Abonnements mit der Zahl der gegenwärtig genutzten Abonnements übereinstimmt.

Sorgen Sie dafür, dass die neuen Abonnements auf der Webseite zur Kontoverwaltung verfügbar sind. Klicken Sie dann auf **Alle erneuern**. Das Bestätigungsfenster fasst zusammen, welche Abonnements erneuert werden. Wenn für einige Maschinen keine identischen Abonnements gefunden werden, haben Sie die Option, den automatischen Vorgang abzubrechen und jedes Abonnement einzeln zu erneuern.

Was bedeutet „Automatisches Erneuern“?

Wenn ein Abonnement endet, wird das nächste Abonnement automatisch aus den verfügbaren Abonnements gewählt, also automatisch erneuert. Das nächste Abonnement muss zum aktuellen Abonnement identisch sein.

Wenn kein identisches Abonnement gefunden wird, erfolgt keine automatische Erneuerung und die Backups könnten fehlschlagen. Es werden keine Abonnements automatisch gekauft. Es können nur Abonnements verwendet werden, die zum Zeitpunkt der automatischen Erneuerung verfügbar sind. Sie können die automatische Erneuerung für jedes einzelne Abonnement wählen oder als Aktion für alle vorhandenen, aktivierten Abonnements.

16.1.10.6 Wie kann die Storage-Quota für eine Maschine erhöht werden?

Ersetzen Sie das der Maschine zugewiesene Abonnement mit einem Abonnement, welches eine größere Storage-Quota hat. Das neue Abonnement muss denselben Typ wie das alte haben. Sie können beispielsweise ein Workstation-Abonnement nur mit einem anderen Workstation-Abonnement ersetzen (welches eine größere Quota hat).

Die Vergrößerung der Storage-Quota ist kostenlos. Die Aktion kann nach ihrem Abschluss nicht mehr rückgängig gemacht werden.

Das neue Abonnement wird einen geringeren Abonnementzeitraum haben. Die Berechnung wird folgendermaßen durchgeführt:

$$Zn = Za * (Qa / Qn)$$

wobei gilt:

- Zn – verbleibender Zeitraum neues Abonnement
- Za – verbleibender Zeitraum altes Abonnement
- Qa – Storage-Quota altes Abonnement
- Qn – Storage-Quota neues Abonnement.

Beispiel: Sie haben ein 250-GB-Abonnement und Sie möchten die Storage-Quota 2 Monate vor Ablauf des Abonnements erhöhen. Die Storage-Quota des neuen Abonnements beträgt 500 GB. Der verbleibende Zeitraum für das neue Abonnement ist daher:

Zn = 2 Monate * (250 GB / 500 GB) = 1 Monat

So erhöhen Sie eine Storage-Quota

1. Gehen Sie zur Webseite der Kontoverwaltung.
2. Wählen Sie die Maschine, für die Sie die Storage-Quota anheben wollen und klicken Sie auf **Vergrößern**.
3. Falls das vorliegende Abonnement bereits die maximal verfügbare Storage Quota für diesen Abonnementtyp hat, zeigt die Software eine entsprechende Meldung an. Wählen Sie anderenfalls die neue Storage-Quota.
4. Klicken Sie auf **Vergrößern** und dann auf **OK**, um die Aktion zu bestätigen.

16.1.10.7 Wofür gibt es die Spalte „Gruppe"?

Damit können Sie solche Aktionen wie **Alle erneuern** oder **Alle automatisch erneuern** auf ausgewählte Abonnements anwenden. Spezifizieren Sie den gewünschten Gruppennamen (beispielsweise Verkaufsabteilung), bei den Abonnements, die Sie gruppieren wollen. Klicken Sie auf den Spaltenkopf **Gruppe**, um die Abonnements zu sortieren und wenden Sie dann die gewünschten Aktionen auf die Gruppe an.

16.1.10.8 Kann ein Abonnement auf einer Maschine widerrufen werden?

Sie können ein einmal aktiviertes Abonnement nicht erneut in die Liste der verfügbaren Abonnements stellen, aber sie können es einer beliebigen Maschine über die Benutzeroberfläche von Acronis Backup & Recovery 11.5 neu zuweisen (S. 478).

16.1.10.9 Können Abonnements gekündigt werden?

Warten Sie einfach, bis das Abonnement abgelaufen ist. Rückerstattungen sind bei Abonnements für Online Backup nicht möglich.

16.2 Was sind meine ersten Schritte?

Melden Sie sich bei Ihrem Konto auf der Acronis-Website an (oder erstellen Sie ein Konto, falls Sie noch nicht registriert sind) und navigieren Sie zu **Online Backup**, **Für Unternehmen**. Das ist die *Webseite zur Kontoverwaltung*. Sie können hier ein Test-Abonnement erhalten, einen Acronis-Partner finden oder ein Abonnement online kaufen. Neu erhaltene Abonnements sind als verfügbare Abonnements in der Registerlasche **Abonnements verwalten** aufgelistet.

Wenn Sie Ihre Abonnements von einem Acronis-Partner erworben haben, dann registrieren Sie diese manuell unter Verwendung des Links '**Neuen Registrierungscode eingeben**'. Der Registrierungscode kommt zusammen mit der Kaufbestätigung per E-Mail.

Danach installieren Sie die Acronis Software (falls noch nicht installiert) und müssen nun jedes Abonnement einer Maschine zuweisen (S. 477). Dadurch werden die Abonnements aktiviert. Sie können anschließend mit dem Backup zum Acronis Online Backup Storage beginnen.

16.3 Abonnement wählen

Abonnements für mehrere Systeme

Ein Abonnement **für mehrere Systeme** ermöglicht Ihnen, eine unbegrenzte Anzahl von physikalischen und/oder virtuellen Maschinen zu sichern. Alle gesicherten Maschinen teilen sich eine gemeinsame Storage-Quota. Der Abonnementzeitraum beginnt mit dem Tag des Erwerbs.

Abonnements pro System

Ein Abonnement **pro System** ermöglicht Ihnen, eine einzelne physikalische Maschine per Backup zu sichern – oder alle virtuelle Maschinen, die von einem Agenten für ESX(i) oder einem Agenten für Hyper-V verwaltet werden. Die Storage-Quota gilt entsprechend für diese physikalische Maschine – oder eben für alle virtuellen Maschinen, die vom Agenten verwaltet werden. Der Abonnementzeitraum beginnt, sobald das Abonnement auf der Maschine aktiviert wurde.

Wählen Sie, basierend auf dem Betriebssystem, welches auf der Maschine läuft, für eine physikalische Maschine den Abonnementtyp **Server** oder **Workstation**. Falls Sie im Zweifel sind, ob es sich bei der Maschine um einen Server oder eine Workstation handelt, dann informieren Sie sich in der Liste der unterstützten Betriebssysteme (S. 462).

Verwenden Sie für virtuelle Maschinen, die vom Agenten für ESX(i) oder dem Agenten für Hyper-V verwaltet werden, das entsprechende Abonnement für **virtuelle Maschinen**. Zusätzlich zur Möglichkeit, Backups der virtuellen Maschinen zu erstellen, können Sie mit diesem Abonnement zudem auch deren physikalischen Host sichern.

Was ist, wenn die Storage-Quota des Abonnements nicht dem von Ihnen benötigten Speicherplatz entspricht?

Wenn es sich abzeichnet, dass Ihre Backups in der Summe größer als die Storage-Quota für das Abonnement sein werden, können Sie ein Abonnement mit größerer Storage-Quota verwenden. Sie können beispielsweise auf einer Workstation auch ein Abonnement für Server oder für virtuelle Maschinen verwenden. Oder Sie können auf einem Server, der kein Virtualisierungsserver ist, auch ein Abonnement für virtuelle Maschinen verwenden.

Die umgekehrte Verwendung ist jedoch nicht möglich. Sie können einen Server nicht mit einem Workstation-Abonnement sichern. Wenn Sie versuchen, virtuelle ESX(i)- oder Hyper-V-Maschinen von einem Host zu sichern, der ein Server-Abonnement verwendet, dann schlägt das Backup fehl.

Test-Abonnements

Sie können ein freies Abonnement pro Konto erhalten. Die Storage-Quota des Testabonnements entspricht der des Standardabonnements. Der Abonnementzeitraum ist auf zwei Monate beschränkt.

Ein Test-Abonnement zu erhalten ist solange möglich, bis Sie ein bezahltes Abonnement eingehen. Sie können ein Test-Abonnement zusammen mit bezahlten Abonnements verwenden. Für Test-Abonnements gelten die gleichen Ablaufregeln wie für bezahlte Abonnements.

Sie können den Dienst nach Ablauf des Testabonnements weiter verwenden, wenn Sie denselben Abonnementtyp erwerben und das Test-Abonnement erneuern, indem Sie das gekaufte Abonnement spezifizieren. Die auf dem Online Storage gesicherten Daten bleiben erhalten. Regelmäßige Backups Ihrer Maschinen werden unterbrechungsfrei fortgesetzt. Ein erneutes Voll-Backup ist nicht nötig.

Gehen Sie folgendermaßen vor, um ein Test-Abonnement zu erhalten:

- Gehen Sie zur Kontenverwaltungs-Webseite, klicken Sie auf **Jetzt für 60 Tage kostenlos testen** und wählen Sie den gewünschten Abonnementtyp.
- Installieren Sie Acronis Backup & Recovery 11.5, starten Sie das Produkt, verbinden Sie die Konsole mit der zu sichernden Maschine, klicken Sie auf **Backup jetzt** oder **Backup-Plan erstellen**, klicken Sie auf **Speicherort** und dann auf **Test-Abonnement erhalten**. Melden Sie sich mit Ihrem Konto an (oder erstellen Sie ein Konto, falls Sie noch nicht registriert sind). Es wird automatisch ein Test-Abonnement erstellt und der Maschine zugewiesen.

16.4 Abonnements für Online Backup aktivieren

Ein Abonnement auf einer Maschine zu aktivieren, bedeutet, der Maschine zu erlauben, Backups zum bzw. im Online Storage zu erstellen.

Ein Abonnement **für mehrere Systeme** wird automatisch aktiviert, sobald Sie damit beginnen, Backups der Maschine zum bzw. in den Acronis Online Backup Storage zu erstellen.

Ein Abonnement **pro System** (für Workstations, Server oder virtuelle Maschinen) muss manuell aktiviert werden. Der entsprechende Abonnementzeitraum beginnt mit dem Augenblick der Aktivierung.

Wichtig! *– Bevor Sie das* erste *Abonnement für Ihre Konto aktivieren, sollten Sie das in Ihrem Profil ausgewählte Land überprüfen. Der Dienst bestimmt abhängig von dieser Ländereinstellung das Datacenter, zu dem Ihre Backup geschickt werden. Stellen Sie sicher, dass Sie das Land wählen, in dem sich alle oder die Mehrheit aller Maschinen befinden, deren Backups Sie zum Online Storage speichern wollen. Ansonsten müssen die Daten über einen unnötig langen Weg verschickt werden. Sie können das Datacenter später nicht mehr ändern, auch dann nicht, wenn Sie das Land in Ihrem Profil ändern. Gehen Sie, um Zugriff auf Ihr Profil zu erhalten, zur Acronis-Website, wählen Sie dort den Bereich* ***Mein Konto****, melden Sie sich an – und klicken Sie anschließend auf* ***Persönliches Profil****.*

16.4.1 Abonnements werden aktiviert

Stellen Sie zu Beginn sicher, dass die Maschinen, deren Abonnements Sie aktivieren möchten, auf dem Management Server registriert und verfügbar sind (eingeschaltet).

Sollten Sie virtuelle ESX(i)-Maschinen sichern wollen, dann binden Sie diese, wie im Abschnitt 'Anbindung des Agenten für ESX(i)' des Dokuments 'Backups von virtuellen Maschinen' beschrieben, an den Agenten für ESX(i). Wählen Sie beim Aktivieren des Abonnements für virtuelle Maschinen diejenige Maschine aus, auf welcher der Agent läuft.

So aktivieren Sie Abonnements

1. Verbinden Sie die Konsole mit dem Management Server.
2. Klicken Sie im Menü **Aktionen** auf **Abonnements für Online Backup aktivieren**
3. Spezifizieren Sie Benutzername und Kennwort zur Anmeldung am Online Storage.
4. Wählen Sie aus der Liste '**Workstations**' oder '**Server**' eine beliebige Anzahl von Maschinen und klicken Sie dann auf **Abonnement wählen**.

5. Wählen Sie den Typ von Abonnements, den Sie für die Maschinen aktivieren wollen. Die Anzahl der Abonnements muss mindestens gleich groß wie die Anzahl an gewählten Maschinen sein.
6. Klicken Sie auf **Jetzt aktivieren**.
7. Führen Sie die letzten drei Schritte für alle anderen Maschinen aus, auf denen Sie Abonnements aktivieren wollen.

Alternativ können Sie ein Abonnement aktivieren, wenn anstelle des Management Servers die Konsole mit der Maschine verbunden ist.

16.4.2 Aktiviertes Abonnement erneut zuweisen

Manchmal möchten Sie vielleicht ein bereits aktiviertes Abonnement anstelle eines verfügbaren Abonnements verwenden. Typische Beispiele wären folgende:

- Sie benötigen bei einer der Maschinen keine Backups mehr und möchten das Abonnement dieser Maschine für ein andere verwenden.
- Sie haben auf einer Maschine Acronis Backup & Recovery 11.5 erneut installiert und möchten deren Online Backups fortsetzen.
- Sie haben die Maschine auf einer fabrikneuen Hardware wiederhergestellt (oder in einem Zustand, in dem noch kein Abonnement aktiviert war) und möchten deren Online Backups fortsetzen.

Wenn Sie ein Abonnement neu zuweisen, beginnt der Abonnementzeitraum nicht von Neuem.

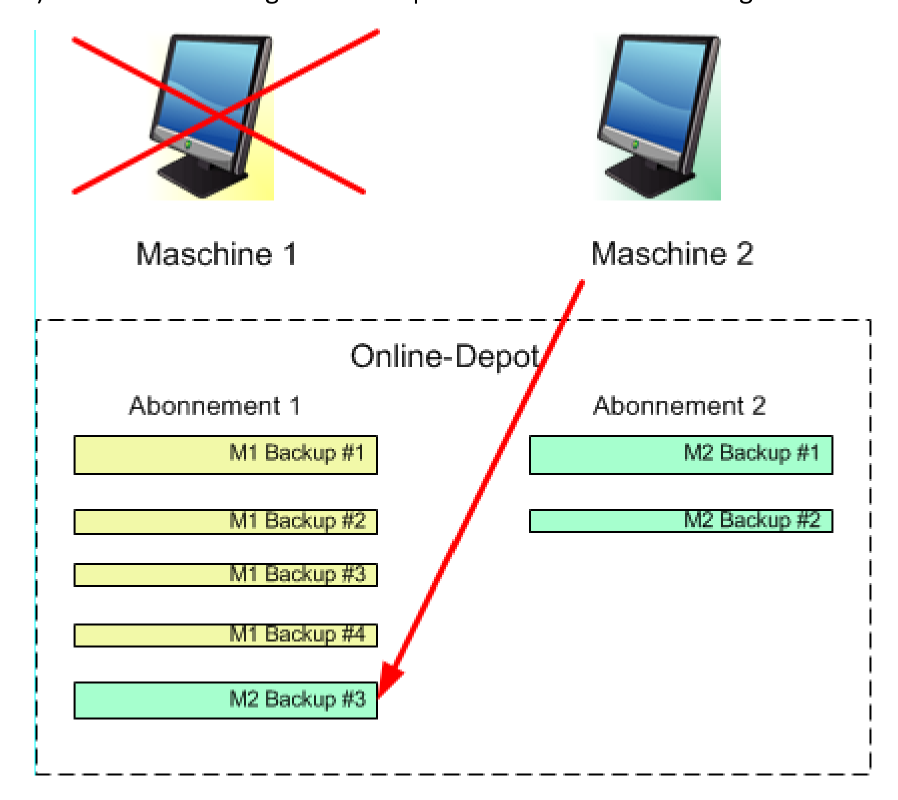
So weisen Sie einer Maschine ein aktiviertes Abonnement zu

1. Gehen Sie auf der Maschine, der Sie ein aktiviertes Abonnement zuweisen möchten, in das Fenster zum Aktivieren des Abonnements.
2. Klicken Sie auf **Ein bereits verwendetes Abonnement neu zuweisen**.
3. Wählen Sie die Maschine, deren Abonnement Sie der aktuellen Maschine neu zuweisen wollen.
4. Klicken Sie auf Jetzt neu zuweisen.

Beispiel

Das untere Diagramm verdeutlicht, was passiert, wenn Sie ein Abonnement einer anderen Maschine neu zuweisen. Angenommen, Maschine 1 hat vier Backups in Abonnement 1. Maschine 2 hat zwei Backups in Abonnement 2. Zu diesem Zeitpunkt weisen Sie das Abonnement 1 auf der Maschine 2 neu zu. Maschine 2 erstellt ihr drittes Backup unter Abonnement 1.

In Abhängigkeit von Ihren Einstellungen wird dieses Backup entweder vollständig oder inkrementell. Seine Größe ist aber vermutlich nicht geringer als die Größe eines Voll-Backups. Es ist daher nicht sinnvoll, ein Abonnement einer Maschine neu zuzuweisen, deren erstes Backup als Initial Seeding durchgeführt wurde. Sie müssen dann entweder das Initial Seeding erneut ausführen (was eine neue Lizenz erfordert) oder das ziemlich große Backup über das Internet übertragen.



Alle früher erstellten Backups verbleiben intakt. Sie können diese bei Bedarf auch manuell löschen. Beachten Sie aber, dass Backups von einem Abonnement nur durch die Maschine gelöscht werden können, der das Abonnement zugewiesen wurde. Sie haben beispielsweise folgende Optionen.

Vor erneuter Zuweisung

Löschen Sie Backups vom Abonnement 1 unter Verwendung von Maschine 1 (sofern verfügbar und angeschaltet). Löschen Sie Backups von Abonnement 2 unter Verwendung von Maschine 2.

Nach erneuter Zuweisung

Löschen Sie Backups von Abonnement 1 unter Verwendung von Maschine 2. Sie können Backups von Abonnement 2 nicht löschen, solange Sie dieses Abonnement keiner anderen Maschine zuweisen.

16.5 Proxy-Einstellungen konfigurieren

Wenn eine oder mehrere Maschinen mit installiertem Agent per Proxy-Server auf das Internet zugreifen, dann müssen Sie jeden entsprechenden Agenten zur Verwendung des Proxy-Servers konfigurieren.

Der Management Server verbindet sich mit dem Internet, um Informationen über die Online-Backup-Abonnements abzurufen. Deshalb müssen die Proxy-Einstellungen auch für den Management Server konfiguriert werden.

Die Proxy-Einstellungen für Agent und Management Server müssen separat konfiguriert werden, auch wenn sie auf derselben Maschine installiert sind.

So konfigurieren Sie die Proxy-Einstellungen für den Agent

1. Verbinden Sie die Konsole mit der Maschine, deren Proxy-Einstellungen Sie konfigurieren wollen.
2. Klicken Sie im Menü **Optionen** auf **Maschinen-Optionen**.
3. Klicken Sie auf **Online Backup-Proxy**.
4. Tragen Sie die Einstellungen für den Proxy-Server ein. Konsultieren Sie die kontextabhängige Hilfe, um detaillierte Informationen (S. 443) zu den Einstellungen zu erhalten.
5. Wiederholen Sie die Schritte 2-4 für alle Maschinen, die per Proxy-Server auf das Internet zugreifen.

So konfigurieren Sie die Proxy-Einstellungen für den Management Server

1. Verbinden Sie die Konsole mit dem Management Server.
2. Klicken Sie im Menü **Optionen** auf **Management Server-Optionen**.
3. Klicken Sie auf **Online Backup-Proxy**.
4. Tragen Sie die Einstellungen für den Proxy-Server ein. Konsultieren Sie die kontextabhängige Hilfe, um detaillierte Informationen (S. 443) zu den Einstellungen zu erhalten.

16.6 Dateien vom Online Storage mit einem Webbrowser abrufen

Sie können durch Verwendung eines Webbrowsers den Acronis Online Backup Storage durchsuchen, den Inhalt von dateibasierten Archiven einsehen sowie ausgewählte Dateien und Ordner herunterladen.

Folgende Browser unterstützen diese Aktionen:

- Internet Explorer 7 oder später
- Mozilla Firefox 3.5 oder später
- Google Chrome 10 oder später
- Safari 5.0.5 oder später

So rufen Sie Dateien vom Online Storage ab:

1. Rufen Sie die Webseite zur Kontenverwaltung (S. 473) auf und klicken Sie auf den Befehl **Dateien aus der Acronis Cloud wiederherstellen**. Ihnen wird die Liste der Maschinen angezeigt, die mit dem spezifizierten Konto gesichert wurden.
2. Klicken Sie auf den Namen der Maschine, deren Daten Sie abrufen wollen. Die Software zeigt Ihnen die Laufwerk- und Datei-Archive an, die die Daten dieser Maschine enthalten.

   Hinweis für Benutzer des Initial Seeding (S. 79)-Dienstes. Ein 'Initial Seeding'-Backup wird zwar von Ihrem (eingesendeten) Festplattenlaufwerk zum Acronis Online Backup Storage hochgeladen und es ist auch sichtbar, seine Daten sind jedoch hier nicht abrufbar.
3. Klicken Sie auf das gewünschte Datei-Archiv. Geben Sie auf Nachfrage das Archivkennwort ein. Die Software zeigt Ihnen alle jemals in dieses Archiv gesicherten Dateien und Ordner an.
4. Wechseln Sie bei Bedarf zum benötigten Ordner oder verwenden Sie die Suchfunktion, um eine Liste der erforderlichen Dateien und Ordner abzurufen.

   Details: Der Suchbefehl kann auch die Platzhalterzeichen (Wildcards) * und ? enthalten.
5. Wählen Sie eine der nachfolgenden Varianten:
   - Um von einer bestimmten Datei oder einem Ordner die jüngste Version zu erhalten, müssen Sie nur auf den entsprechenden Namen klicken.

- Um von mehreren Dateien und Ordnern die jüngsten Versionen zu erhalten, aktivieren Sie die links danebenliegenden Kontrollkästchen und klicken Sie dann auf die Schaltfläche **Recovery**.
- Um von einer Datei oder einem Ordner eine frühere Version zu erhalten, klicken Sie auf das rechts danebenliegende Icon (⚙) und wählen Sie dann den Befehl **Versionen anzeigen**. Daraufhin öffnet sich ein Fenster mit einer Versionsliste. Wählen Sie in diesem Fenster die gewünschte Version anhand von Datum sowie Uhrzeit aus und klicken Sie dann auf den Befehl **Recovery**.
- [Bei Verwendung der Suche nicht verfügbar] Um frühere Versionen von mehreren Dateien und Ordnern abzurufen, wählen Sie den gewünschten Zeitpunkt aus der Liste **Versionen**. Aktivieren Sie die Kontrollkästchen links neben den Dateien bzw. Ordnern und klicken Sie dann auf die grüne Schaltfläche **Recovery**.

  Details: Sie erhalten diejenigen Datei- bzw. Ordner-Versionen, die vor und möglichst nah zu dem gewählten Zeitpunkt per Backup gesichert wurden.

6. Klicken Sie auf **Speichern**, um die ausgewählten Dateien herunterzuladen.

   Details: Falls Sie eine einzelne Datei ausgewählt haben, wird diese wie vorliegend heruntergeladen. Ansonsten werden die gewählten Daten in eine .zip-Datei archiviert (mit dem vorgegebenen Namen 'AcronisArchive.zip').
7. Wählen Sie den Ort, wo die Daten abgelegt werden sollen und klicken Sie auf **Speichern**.

16.7 Beschränkungen des Online Storages

Abweichend von anderen, ebenfalls in Acronis Backup & Recovery 11.5 verfügbaren Storages hat der Online Storage folgende Einschränkungen.

Aktionen

Folgende Aktionen sind nicht möglich.

Backup-Aktionen:

- Backup mit einem bootfähigen Medium
- Backup unter Linux
- Backup mit dem Agenten für Microsoft Exchange-Server
- Erstellen differentieller Backups
- Verwendung des Backup-Schemas **Benutzerdefiniert**
- Vereinfachte Benennung von Backup-Dateien
- Simultanes, Host-basiertes Backup von mehreren virtuellen Maschinen
- Regelmäßige Konvertierung von Backups zu einer virtuellen Maschine einrichten

'**Aktionen mit Backups**':

- Ein Backup validieren*
- Backup exportieren
- Backup mounten
- Backups *vom* Online Storage aus replizieren oder verschieben
- Ein inkrementelles Backup zu einem vollständigen konvertieren

Aktionen mit Archiven (ein Archiv ist eine Zusammenstellung von Backups):

- Ein Archiv validieren

- Ein Archiv exportieren

Diese Einschränkungen gelten auch für Backups mit Initial Seeding bzw. Wiederherstellungen mit Large Scale Recovery.

* Ein 'Initial Seeding'-Backup wird direkt nach seiner Erstellung automatisch validiert.

Backup- und Recovery-Optionen

Einige Backup- und Recovery-Optionen werden bei Online Backups nicht unterstützt. Beispielsweise **Backup-Aufteilung** (S. 121).

Durch Verwendung der Option '**Backup-Performance –> Netzwerkverbindungsgeschwindigkeit**' können Sie die Übertragungsrate in Kilobyte pro Sekunde (aber nicht in Prozent) variieren.

16.8 Terminologiereferenz

Nachfolgend finden Sie einige Begriffe in Bezug auf Acronis Backup & Recovery Online.

Ein Abonnement aktivieren

Ermöglicht der Maschine, den Online Storage in Übereinstimmung mit dem Abonnement zu verwenden.

Aktiviertes Abonnement

Ein Abonnement, das aktuell von einer Maschine verwendet wird.

Ein Abonnement einer Maschine zuweisen

Reservieren Sie ein Abonnement für eine bestimmte Maschine, um dessen aktuelles Abonnement zu erneuern.

Zugewiesenes Abonnement

Ein Abonnement, welches einer Maschine zugewiesen wurde.

Verfügbares Abonnement

Ein Abonnement, welches noch keiner Maschine zugewiesen wurde.

Extra-Service

Ein Dienst, den Sie zusätzlich zu Abonnements für Online Backup verwenden können.

Die Storage-Quota vergrößern

Ersetzen Sie ein Abonnement durch ein anderes, das über eine größere Storage-Quota verfügt. Der verbleibende Abonnementzeitraum wird im Verhältnis zur vergrößerten Kapazität herabgesetzt.

Initial Seeding

Initial Seeding ist ein Extra-Service, bei dem Sie das anfängliche Voll-Backup lokal ausführen und dieses dann per Festplatte (oder mit einem vergleichbaren Laufwerk) an Acronis senden. Acronis lädt das Backup dann zum Online Storage hoch. Danach können Sie dieses Voll-Backup – manuell oder nach Zeitplan – mit nachfolgenden inkrementellen Backups erweitern.

Der 'Initial Seeding'-Dienst ist in Ihrer Region möglicherweise nicht verfügbar. Klicken Sie hier für weitere Informationen: http://kb.acronis.com/content/15118.

Large Scale Recovery

Large Scale Recovery ist ein Extra-Service, mit dem Sie eine Kopie der Backups erhalten, welche sich im Online Storage befinden. Anschließend können Sie die Daten aus dieser Kopie wiederherstellen.

Der 'Large Scale Recovery'-Dienst ist in Ihrer Region möglicherweise nicht verfügbar. Klicken Sie hier für weitere Informationen: http://kb.acronis.com/content/15118.

Lizenz

Nicht zu verwechseln mit Produktlizenzen von Acronis Backup & Recovery 11.5.

Erlaubnis für eine Maschine, einen Extra-Service von Acronis Backup & Recovery Online zu verwenden.

Sie können 'Initial Seeding'-Lizenzen bzw. 'Large Scale Recovery'-Lizenzen erwerben.

Ein Abonnement neu zuweisen

Ein bereits aktiviertes Abonnement einer anderen Maschine zuweisen.

Registrierungscode

Zeichenkette zur Registrierung eines Abonnements oder einer Lizenz, die bei einem Acronis-Partner erworben wurde.

Wenn Sie ein solches Abonnement oder eine solche Lizenz erworben haben, erhalten Sie eine Bestätigungs-E-Mail mit den Registrierungscodes für jede von diesen. Danach tragen Sie diese Registrierungscodes auf der Webseite zur Kontoverwaltung ein – worauf diese Abonnements und Lizenzen zur Benutzung verfügbar werden.

Ein Abonnement erneuern

Weisen Sie ein Abonnement des gleichen Typs zu – und mit der gleichen oder einer größeren Storage Quota, als die des derzeitigen, aktivieren Abonnements.

Dieses Abonnement wird aktiviert, sobald das aktuelle Abonnement endet.

Storage-Quota

Die Menge an Speicherplatz auf dem Online Storage, die auf Basis des Abonnements belegt werden kann.

Abonnement

Erlaubnis für eine oder mehrere Maschinen, eine bestimmte Menge an Speicherplatz für eine bestimmte Zeitdauer auf dem Online Storage zu verwenden.

Abonnementzeitraum

Zeitraum, in dem ein Abonnement aktiviert bleibt. Sie können die Maschine während dieses Zeitraums sichern und wiederherstellen. Eine Wiederherstellung ist auch noch für weitere 30 Tage nach Ablauf des Zeitraums möglich.

Eine Abonnement-Zuweisung aufheben

Macht ein bereits zugewiesenes Abonnement wieder verfügbar.

Sie können die Zuweisung eines Abonnements aufheben, so lange es nicht aktiviert wurde.

17 Glossar

A

Acronis Active Restore

Geschützte Technologie von Acronis, die ein System sofort verfügbar macht, nachdem die Wiederherstellung des Systems angefangen hat. Das System bootet aus dem Backup (S. 489) und die Maschine wird betriebsbereit, um notwendige Dienste zur Verfügung zu stellen. Die für eingehende Anforderungen notwendigen Daten werden mit der höchsten Priorität, alle anderen im Hintergrund wiederhergestellt. Beschränkungen:

- das Backup muss sich auf einem lokalen Laufwerk befinden (irgendeinem Gerät, das durch das BIOS verfügbar gemacht wird mit Ausnahmen des Bootens über das Netzwerk)
- Linux-Images werden nicht unterstützt
- GPT-Laufwerke und der UEFI-Boot-Modus werden nicht unterstützt.

Acronis Plug-in für WinPE

Modifikation von Acronis Backup & Recovery 11.5 Agent für Windows, die in einer Preinstallation Environment ausgeführt werden kann. Das Plugin kann mit Hilfe von Bootable Media Builder zu einem Image für WinPE (S. 497) hinzugefügt werden. Die resultierenden bootfähigen Medien (S. 487) können benutzt werden, jede PC-kompatible Maschine zu starten – und, mit gewissen Einschränkungen, die meisten direkten Verwaltungsaufgaben (S. 489) ohne Hilfe des Betriebssystems auszuführen. Aktionen können entweder lokal über die Benutzerschnittstelle oder remote mit Hilfe der Konsole (S. 492) konfiguriert und gesteuert werden.

Acronis Secure Zone

Ein geschütztes Volume zum Speichern von Backup-Archiven (S. 485) innerhalb einer verwalteten Maschine (S. 496). Vorteile:

- ermöglicht die Wiederherstellung eines Laufwerks auf dasselbe Laufwerk, auf der auch die Laufwerk-Backups hinterlegt sind
- bietet eine kosteneffektive und handliche Methode zum Schutz vor Softwarefehlern, Virusangriffen, Bedienerfehlern
- beseitigt die Notwendigkeit, in jedem Fall für Backup oder Wiederherstellung ein separates Medium oder eine Netzwerkverbindung bereitstellen zu müssen. Diese Funktion ist besonders für mobile Benutzer nützlich.
- kann als primärer Speicherort dienen, von wo aus Backups dann weiter repliziert werden.

Einschränkung: die Acronis Secure Zone kann nicht auf einem dynamischen Laufwerk (S. 490) organisiert werden.

Die Acronis Secure Zone wird als persönliches Depot (S. 494) betrachtet.

Acronis Startup Recovery Manager (ASRM)

Eine Modifikation des bootfähigen Agenten (S. 487), auf dem Systemlaufwerk liegend und konfiguriert, um beim Booten zu starten, wenn die Taste F11 gedrückt wird. Acronis Startup Recovery Manager bietet eine Alternative zu Rettungsmedien oder einer Netzwerkverbindung, um ein bootfähiges Rettungswerkzeug zu starten.

Der Acronis Startup Recovery Manager ist besonders für mobile Anwender nützlich. Wenn ein Fehler auftritt, bootet der Benutzer die Maschine neu, drückt die F11-Taste, sobald die Meldung „Druecken Sie F11 zum Ausfuehren des Acronis Startup Recovery Managers…“ erscheint, und stellt dann die Daten auf die gleiche Weise wie mit den gewöhnlichen bootfähigen Medien wieder her.

Einschränkungen: Erfordert die Reaktivierung von Boot-Loadern außer Windows-Loadern und GRUB.

Acronis Universal Restore

Eine proprietäre Acronis-Technologie, um Windows oder Linux auf abweichender Hardware oder einer virtuellen Maschine bootfähig zu machen. Universal Restore handhabt Abweichungen bei Geräten, die kritisch für den Betriebssystemstart sind, wie beispielsweise Speicher-Controller, Hauptplatine oder Chipsatz.

Universal Restore ist nicht verfügbar:

- wenn das wiederherzustellende Image in der Acronis Secure Zone (S. 484) liegt oder
- wenn Acronis Active Restore (S. 484) verwendet wird,

weil alle diese Funktionen in erster Linie zur sofortigen Datenwiederherstellung auf der gleichen Maschine gedacht sind.

Agent (Acronis Backup & Recovery 11.5 Agent)

Anwendung, die das Backup und die Wiederherstellung von Daten und andere Verwaltungsaufgaben auf der Maschine (S. 493) ermöglicht, wie z.B. die Task-Verwaltung und Aktionen mit Festplatten.

Die Art Daten, die gesichert werden können, hängt vom Typ des Agenten ab. Acronis Backup & Recovery 11.5 enthält die Agenten für das Backup von Festplatten und Dateien und die Agenten für das Backup virtueller Maschinen, die auf Virtualisierungs-Servern bereitgestellt werden.

Aktivität

Eine von Acronis Backup & Recovery 11.5 durchgeführte Aktion, die dem Erreichen eines bestimmten, vom Benutzer gesteckten Ziels dient. Beispiele: Backup, Recovery, Export eines Backups, Katalogisierung eines Depots. Eine Aktivität kann durch einen Benutzer oder die Software selbst initiiert werden. Die Ausführung eines Tasks (S. 495) verursacht immer eine oder mehrere Aktivitäten.

Archiv

Siehe Backup-Archiv (S. 486).

Aufbewahrungsregeln

Der Teil eines Backup-Plans (S. 486), der spezifiziert, wann und wie von diesem Plan erstellte Backups (S. 485) gelöscht oder verschoben werden sollen.



Backup

Ein Backup ist das Ergebnis einer einzelnen Backup-Aktion. Physikalisch gesehen handelt es sich um eine Datei oder Bandaufzeichnung, die eine Kopie der gesicherten Daten zu einem spezifischen

Zeitpunkt enthält. Backup-Dateien, die von Acronis Backup & Recovery 11.5 erstellt wurden, haben die Dateierweiterung tib. TIB-Dateien, die das Ergebnis eines Backup-Exports (S. 491) oder Konsolidierung (S. 492) sind, werden ebenfalls als Backups bezeichnet.

Backup (Aktion)

Aktion, die eine Kopie der Daten erstellt, die auf der Festplatte einer Maschine (S. 493) existieren, um diese wiederherzustellen oder in den Zustand zu einem festgelegten Tag bzw. Zeitpunkt zurückzusetzen.

Backup-Archiv (Archiv)

Satz von Backups (S. 485), die mit einem Backup-Plan (S. 486) erstellt und verwaltet werden. Ein Archiv kann mehrere Voll-Backups (S. 497) enthalten, aber auch inkrementelle (S. 492) und differentielle Backups (S. 489). Backups, die zum gleichen Archiv gehören, werden immer am gleichen Ort gespeichert. Falls ein Backup-Plan eine Replikation (S. 494) oder Verschiebung von Backups zu weiteren Speicherorten beinhaltet, dann bilden die Backups an jedem dieser Speicherorte ein separates Archiv.

Backup-Optionen

Konfiguration der Parameter für eine Backup-Aktion, wie zum Beispiel die Befehle vor bzw. nach dem Backup, die maximale Bandbreite im Netzwerk, die dem Backup zugeteilt wird, oder die Datenkomprimierungsrate. Backup-Optionen sind Bestandteil eines Backup-Plans (S. 486).

Backup-Plan (Plan)

Ein Satz von Regeln, der spezifiziert, wie gegebene Daten auf einer bestimmten Maschine geschützt bzw. gesichert werden sollen. Ein Backup-Plan spezifiziert:

- welche Daten gesichert werden sollen
- den Namen und Speicherort des Backup-Archivs (S. 486)
- das Backup-Schema (S. 487). Das schließt eine Backup-Planung und [optional] Aufbewahrungsregeln (S. 485) mit ein
- [optional] zusätzliche Aktionen, die mit den Backups durchgeführt werden sollen (Replikation (S. 494), Validierung (S. 496), Konvertierung zu einer virtuellen Maschine)
- die Backup-Optionen (S. 486).

Ein Backup-Plan kann beispielsweise folgende Informationen enthalten:

- führe ein Backup von Volume C: aus **(das sind die Daten, die der Plan schützt)**
- benenne das Archiv 'MeinSystemVolume' und speichere es in '\\server\backups' **(Name und Speicherort des Backup-Archivs)**
- führe ein monatliches Voll-Backup am letzten Tag des Monats um 10:00 Uhr aus und ein inkrementelles Backup an Sonntagen um 22:00 Uhr. Lösche Backups, die älter sind als 3 Monate **(das ist das Backup-Schema)**
- validiere das letzte Backup unmittelbar nach seiner Erstellung **(das ist die Validierungsregel)**
- schütze das Archiv mit einem Kennwort **(das ist eine Option)**.

Physikalisch ist ein Backup-Plan ein Zusammenstellung von Tasks (S. 495), die auf einer verwalteten Maschine (S. 496) ausgeführt werden.

Ein Backup-Plan kann direkt auf der Maschine erstellt werden, von einer anderen Maschine importiert werden (lokaler Plan) oder vom Management Server auf die Maschine verbreitet werden (zentraler Plan (S. 498)).

Backup-Schema

Teil eines Backup-Plans (S. 486), der den Zeitplan für das Backup und [optional] die Aufbewahrungsregeln und den Zeitplan für die Bereinigung (S. 487) mit einschließt. Beispielsweise führe monatlich ein Voll-Backup (S. 497) am letzten Tag des Monats um 10:00 Uhr aus – und ein inkrementelles Backup (S. 492) an Sonntagen um 22:00 Uhr. Lösche Backups, die älter sind als 3 Monate. Prüfe auf solche Backups jedes Mal, wenn ein Backup abgeschlossen wurde.

Acronis Backup & Recovery 11.5 bietet die Möglichkeit, bekannte optimierte Backup-Schemata wie zum Beispiel GVS und Türme von Hanoi zu verwenden, benutzerdefinierte Backup-Schemata zu erstellen oder alle Daten auf einmal zu sichern.

Bereinigung

Löschen von Backups (S. 485) aus einem Backup-Archiv (S. 486) oder Verschieben zu einem anderen Speicherort, um veraltete Backups zu entfernen oder um zu verhindern, dass das Archiv die gewünschte Größe zu überschreitet.

Eine Bereinigung besteht in derAnwendung von Aufbewahrungsregeln (S. 485) auf ein Archiv. Die Aufbewahrungsregeln werden durch den Backup-Plan (S. 486) eingerichtet, der das Archiv produziert. Eine Bereinigung kann (muss aber nicht) dazu führen, dass Backups gelöscht oder verschoben werden, je nachdem, ob die Aufbewahrungsregeln verletzt wurden oder nicht.

Bootable Agent

Bootfähiges Wiederherstellungswerkzeug, das die meisten Funktionen von Acronis Backup & Recovery 11.5 Agent (S. 485) enthält. Der bootfähige Agent basiert auf einem Linux-Kernel. Eine Maschine (S. 493) kann entweder mit Hilfe bootfähiger Medien (S. 487) oder über den Acronis PXE Server in den bootfähigen Agenten gestartet werden. Aktionen können entweder lokal über die Benutzerschnittstelle oder remote mit Hilfe der Konsole (S. 492) konfiguriert und gesteuert werden.

Bootfähiges Medium

Physikalisches Medium (CD, DVD, USB-Sticks oder andere von einer Maschine (S. 493) als Boot-Gerät unterstützt Medien), die den bootfähigen Agenten (S. 487) oder die Windows Preinstallation Environment (WinPE) (S. 497) mit dem Acronis Plug-in für WinPE (S. 484) enthalten. Eine Maschine kann außerdem mit einer der genannten Umgebungen gestartet werden, wenn die Möglichkeit genutzt wird, per Acronis PXE-Server oder Windows Deployment Service (WDS) über das Netzwerk zu booten. Diese Server mit ihren hochgeladenen, bootfähigen Komponenten können auch als eine Art bootfähiges Medium angesehen werden.

Bootfähige Medien werden am häufigsten verwendet, um:

- ein Betriebssystem wiederherzustellen, das nicht mehr bootet
- auf Daten zuzugreifen und zu sichern, die in einem beschädigten System überlebt haben
- ein Betriebssystem auf fabrikneue Computer zu verteilen
- Basis-Volumes oder dynamische Volumes (S. 491) auf fabrikneuen Festplatten (bzw. ähnlichen Laufwerken) einzurichten
- Laufwerke mit nicht unterstütztem Dateisystem per Sektor-für-Sektor-Backup zu sichern

- Daten 'offline' zu sichern, die wegen einer Zugangsbeschränkung, einer Sperrung durch laufende Anwendungen oder wegen anderer Gründe nicht 'online' gesichert werden können.

D

Datenkatalog

Der Datenkatalog ermöglicht Benutzern, die benötigten Versionen bestimmter Daten leicht zu finden und diese für eine Recovery-Aktion auszuwählen. Benutzer können auf einer verwalteten Maschine (S. 496) Daten in jedem Depot (S. 489), auf das von dieser Maschine Zugriff besteht, einsehen und suchen. Der auf dem Management Server (S. 493) verfügbare zentrale Katalog enthält alle auf seinen Storage Nodes (S. 495) gespeicherten Daten.

Physikalisch wird der Datenkatalog in Katalogdateien gespeichert. Jedes Depot verwendet seinen eigenen Satz an Katalogdateien, die normalerweise direkt im Depot vorliegen. Sollte dies nicht möglich sein, wie etwa bei Band-Storages, dann werden die Katalogdateien in einem lokalen Ordner der verwalteten Maschine oder des Storage Nodes gespeichert. Ein Storage Node speichert zudem die Katalogdateien seiner Remote-Depots auch lokal, um so einen schnelleren Zugriff zu erreichen.

Datenträgergruppe

Anzahl dynamischer Laufwerke (S. 490), die ihre Konfigurationendaten in ihren LDM-Datenbanken speichern und deshalb als ein Ganzes verwaltet werden können. Normalerweise sind alle dynamischen Datenträger, die innerhalb der gleichen Maschine (S. 493) erstellt wurden, Mitglieder der gleichen Datenträgergruppe.

Sobald das erste dynamische Datenträger vom LDM oder einem anderen Festplattenverwaltungswerkzeug erstellt wird, kann der Name der Datenträgergruppe im Registry-Key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\dmio\Boot Info\Primary Disk Group\Name gefunden werden.

Das nächste erstellte oder importierte Datenträger wird zur gleichen Datenträgergruppe hinzugefügt. Die Gruppe existiert, so lange wenigstens eine ihrer Mitglieder existiert. Nachdem der letzte dynamische Datenträger abgeschaltet oder in einen Basisdatenträger konvertiert wurde, ist die Gruppe stillgelegt, obwohl der Name im oben genannten Registry-Key erhalten bleibt. Falls erneut ein dynamischer Datenträger erstellt oder wieder angeschlossen wird, wird eine Datenträgergruppe mit einem inkrementellen Namen erstellt.

Wenn eine Datenträgergruppe zu einer anderen Maschine verschoben wird, wird sie als „fremd“ betrachtet und kann nicht benutzt werden, bis sie in eine existierende Datenträgergruppe importiert wird. Der Import aktualisiert die Konfigurationsdaten auf den lokalen und den 'fremden' Datenträgern, damit sie eine Einheit bilden. Eine 'fremde' Gruppe wird importiert, wie sie ist (wird den ursprünglichen Namen haben), wenn keine Datenträgergruppe auf der Maschine existiert.

Weitere Informationen über Datenträgergruppen finden Sie auf den Microsoft-Webseiten:

222189 Beschreibung der Datenträgergruppen in der Windows Datenträgerverwaltung http://support.microsoft.com/kb/222189/de

Deduplizierendes Depot

Verwaltetes Depot (S. 496) mit aktivierter Deduplizierung (S. 488).

Deduplizierung

Methode, um identische Informationen in verschiedenen Kopien nur einmalig zu speichern.

Acronis Backup & Recovery 11.5 kann die Deduplizierungstechnologie auf Backup-Archive (S. 486) anwenden, die auf Storage Nodes (S. 495) gespeichert sind. Das reduziert den für Archive benötigten Speicherplatz, den Backup-Datentransfer sowie die Netzwerkauslastung während der Backup-Erstellung.

Depot

Ort für die Ablage von Backup-Archiven (S. 486). Ein Depot kann auf einem lokalen Laufwerk, auf einem Netzlaufwerk oder auf einem entfernbaren Medium wie einem USB-Laufwerk organisiert werden. Es gibt keine Limits für die Größe eines Depots oder die Zahl der Backups in einem Depot. Sie können die Größe jedes Archivs durch Bereinigung (S. 487) begrenzen, aber die Gesamtgröße der Archive in einem Depot wird nur durch die Größe des Speichers selbst begrenzt.

Desaster-Recovery-Plan (DRP)

Ein Dokument, die eine Liste von per Backup gesicherten Datenelementen sowie genaue Anweisungen enthält, wie diese Elemente aus dem Backup wiederhergestellt werden sollen.

Wird die entsprechende Backup-Option (S. 486) aktiviert, dann wird ein DRP erstellt, sobald das erste Backup erfolgreich vom Backup-Plan durchgeführt wurde – und ebenso, wenn sich die Liste der Datenelemente oder die DRP-Parameter ändern sollten. Dein DRP kann an die spezifizierten E-Mail-Adressen gesendet oder als Datei in einem lokalen Ordner oder Netzwerkordner gespeichert werden.

Differentielles Backup

Ein differentielles Backup speichert Änderungen an den Daten im Vergleich zum letzten vorangegangenen Voll-Backup (S. 497). Sie benötigen den Zugriff auf das entsprechende Voll-Backup, um die Daten aus einem differentiellen Backup wiederherzustellen.

Direkte Verwaltung

Eine Aktion, die auf einer verwalteten Maschine (S. 496) unter Verwendung einer direkten Verbindung zwischen Konsole (S. 492) und Agent (S. 485) ausgeführt wird (im Gegensatz zur zentraler Verwaltung (S. 497), bei der Aktionen auf dem Management Server (S. 493) konfiguriert und dann durch den Server auf die verwalteten Maschinen verbreitet werden).

Die direkten Verwaltungsaktionen umfassen:

- Erstellung und Verwaltung lokaler Backup-Pläne (S. 493)
- Erstellung und Verwaltung lokaler Tasks (S. 493), wie z.B. Recovery-Tasks
- Erstellung und Verwaltung persönlicher Depots (S. 494) und der dort gespeicherten Archive
- Anzeige der Stadien, Fortschritte und Eigenschaften derjenigen zentralen Tasks (S. 498), die auf der Maschine vorkommen
- Anzeige und Verwaltung von Logs der Aktionen des Agenten
- Laufwerksverwaltungsaktionen wie das Klonen eines Laufwerks sowie das Erstellen und Konvertieren von Volumes.

Bei Verwendung von bootfähigen Medien (S. 487) erfolgt auch eine Art direkte Verwaltung.

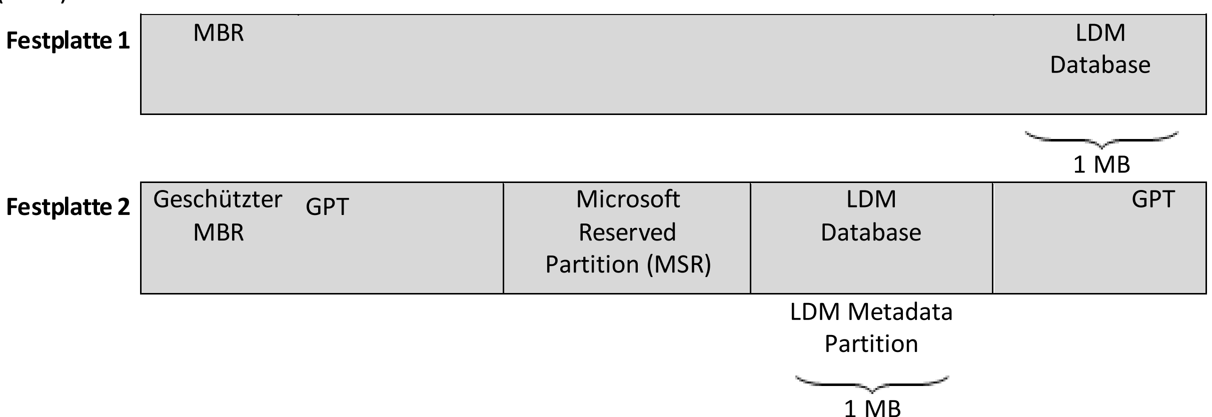
Disk-Backup (Image)

Backup (S. 485), das eine auf den Sektoren basierende Kopie einer Festplatte oder Partition in gepackter Form enthält. Normalerweise werden nur Sektoren kopiert, die Daten enthalten. Acronis Backup & Recovery 11.5 bietet aber eine Option, um Raw-Images zu erstellen, d.h. alle Sektoren zu kopieren, um z.B. das Imaging nicht unterstützter Dateisysteme zu ermöglichen.

Dynamische Festplatten

Laufwerk, das vom Logical Disk Manager (LDM) verwaltet wird, der in Windows seit Windows 2000 verfügbar ist. LDM unterstützt die flexible Zuweisung von Volumes auf einem Speichergerät für bessere Fehlertoleranz, bessere Leistung oder eine höhere Volume-Größe.

Ein dynamisches Laufwerk kann entweder das Partitionierungsschema 'Master Boot Record' (MBR) oder 'GUID-Partitionstabelle' (GPT) verwenden. Zusätzlich zu MBR oder GPT hat jedes dynamische Laufwerk eine versteckte Datenbank, wo der LDM die Konfiguration der dynamischen Volumes speichert. Jedes dynamische Laufwerk hält für eine bessere Speicherzuverlässigkeit die vollständigen Informationen über alle dynamischen Laufwerke bereit, die in der Datenträgergruppe existieren. Die Datenbank besetzt das letzte Megabyte einer MBR-Festplatte. Auf einer GPT-Festplatte erstellt Windows eine dedizierte LDM-Metadaten-Partition, die Platz von der Microsoft Reserved Partition (MSR) entnimmt.



Organisation dynamischer Festplatten auf Basis MBR (Festplatte 1) und GPT (Festplatte 2).

Weitere Informationen über dynamische Datenträger finden Sie im Artikel der Microsoft Knowledgebase:

Disk Management (Windows XP Professional Resource Kit) http://technet.microsoft.com/de-de/library/bb457110.aspx

816307 Empfohlene Verfahrensweisen für die Verwendung dynamischer Datenträger auf Windows Server 2003-Computern http://support.microsoft.com/kb/816307/de.

Dynamische Gruppe

Gruppe von Maschinen (S. 493), die automatisch vom Management Server (S. 493) gemäß der Kriterien für die Mitgliedschaft aufgefüllt wird, die vom Administrator angegeben werden. Acronis Backup & Recovery 11.5 bietet folgende Mitgliedschaftskriterien:

- Betriebssystem
- Active Directory-Organisationseinheit
- IP-Adressbereich

- In txt/csv-Datei aufgelistet.

Eine Maschine verbleibt in einer dynamischen Gruppe, solange die Maschine die Kriterien der Gruppe erfüllt. Der Administrator kann jedoch Ausschließungen spezifizieren und so gewisse Maschinen nicht in der dynamischen Gruppe enthalten sein lassen, auch wenn sie die Kriterien erfüllen.

Dynamisches Volume

Volume, das sich auf auf einem dynamischen Datenträger (S. 490) oder genauer auf einer Datenträgergruppe (S. 488) befindet. Dynamische Volumes können sich über mehrere Laufwerke erstrecken. Dynamische Datenträger sind gewöhnlich abhängig vom gewünschten Ziel gestaltet:

- um die Größe zu erweitern (übergreifendes Volume)
- um die Zugriffszeit zu verringern (Stripesetvolume)
- um die Fehlertoleranz durch redundante Informationen zu erreichen (gespiegelte und RAID-5-Volumes).

E

Exportieren

Eine Aktion, bei der eine Kopie bzw. unabhängige Teilkopie eines Archivs (S. 486) am von Ihnen angegebenen Speicherort erstellt wird. Ein Export kann ein einziges Archiv, ein einziges Backup (S. 485) oder eine Auswahl von Backups aus dem gleichen Archiv umfassen. Ein vollständiges Depot (S. 489) kann über die Befehlszeilenschnittstelle exportiert werden.



GVS (Großvater-Vater-Sohn)

Populäres Backup-Schema (S. 487), das für ein ideales Gleichgewicht zwischen der Größe eines Backup-Archivs (S. 486) und der Anzahl von Wiederherstellungspunkten (S. 497) sorgen soll, die im Archiv enthalten sind. GVS ermöglicht ein Recovery mit täglicher Rasterung für die letzten Tage, wöchentlicher Rasterung für die letzten Wochen und monatlicher Rasterung für jede Zeit in der Vergangenheit.

Weitere Informationen finden Sie bei Backup-Schema GVS.

I

Image

Gleichbedeutend mit Disk-Backup (S. 489).

Indizierung

Eine Aktivität (S. 485), von einem Storage Node (S. 495) durchgeführt, nachdem ein Backup (S. 485) zu einem deduplizierenden Depot (S. 488) gespeichert wurde.

Der Storage Node führt während der Indizierung folgende Aktionen aus:

- Er verschiebt Datenblöcke von dem Backup zu einer speziellen Datei innerhalb des Depots. Diese Datei wird Deduplizierungsdatenspeicher genannt.

- In dem Backup werden die verschobenen Blöcke durch ihre 'Fingerabdrücke' (Hash-Werte) ersetzt.
- Er speichert die Hash-Werte und die Links, die zum Zusammensetzen der deduplizierten Daten notwendig sind, in der Deduplizierungsdatenbank.

Eine Indizierung kann man sich als 'Deduplizierung am Ziel' vorstellen – im Gegensatz zur 'Deduplizierung an der Quelle', welche der Agent (S. 485) während einer Backup-Aktion ausführt. Ein Benutzer kann die Indizierung anhalten und wieder neu aufnehmen.

Inkrementelles Backup

Ein Backup (S. 485), das Datenänderungen in Bezug zum letzten Backup speichert. Sie müssen auf andere Backups des gleichen Archivs (S. 486) zugreifen können, um Daten aus einem inkrementellen Backup wiederherstellen zu können.



Katalogisierung

Beim Katalogisieren eines Backups (S. 485) werden dessen Inhalte zum Datenkatalog (S. 488) hinzugefügt. Backups werden automatisch katalogisiert, sobald Sie erstellt wurden. Backups, die auf einem Storage Node (S. 495) gespeichert sind, werden automatisch durch den Knoten katalogisiert. Backups, die irgendwo anders gespeichert sind, werden durch den Agenten (S. 485) katalogisiert. Der Benutzer kann in den Backup-Optionen (S. 486) zwischen vollständiger und schneller Katalogisierung wählen. Die vollständige Katalogisierung kann außerdem auch manuell gestartet werden.

Konsole (Acronis Backup & Recovery 11.5 Management Console)

Werkzeug für den Remote- oder lokalen Zugriff auf Acronis Agenten (S. 485) und den Acronis Backup & Recovery 11.5 Management Server (S. 493).

Wenn die Konsole mit dem Management Server verbunden ist, kann der Administrator zentrale Backup-Pläne (S. 498) einrichten sowie auf andere Funktionen des Management-Servers zugreifen, d.h. er arbeitet mit zentraler Verwaltung (S. 497). Wenn der Administrator eine direkte Verbindung zwischen Konsole und Agent herstellt, arbeitet er mit direkter Verwaltung (S. 489).

Konsolidierung

Kombinieren zweier oder weiterer subsequenter Backups (S. 485), die zum gleichen Archiv (S. 486) gehören, in ein Backup.

Konsolidierung könnte beim Löschen von Backups gebraucht werden, entweder manuell oder während der Bereinigung (S. 487). Zum Beispiel könnten die Aufbewahrungsregeln erfordern, ein abgelaufenes Voll-Backup (S. 497) zu löschen, aber die nächste inkrementelle Sicherung (S. 492) zu erhalten. Die Backups werden in ein einzelnes Voll-Backup kombiniert und mit dem Datum des inkrementellen Backups versehen. Da die Konsolidierung viel Zeit und Systemressourcen beansprucht, bieten die Aufbewahrungsregeln eine Option, Backups mit Abhängigkeiten nicht zu löschen. Im Beispiel wird das Voll-Backup erhalten, bis auch das inkrementelle Backup veraltet ist. Dann werden beide Backups gelöscht.

L

Logisches Volume

Dieser Begriff hat zwei Bedeutungen, abhängig vom Kontext.

- Ein Volume, dessen Information in einer erweiterten Partitionstabelle gespeichert wird. (Im Gegensatz zu einem primären Volume, dessen Information im Master Boot Record gespeichert wird).
- Ein Volume, das unter Verwendung des Logical Volume Managers (LVM) des Linux-Kernels erstellt wurde. LVM gibt einem Administrator die Flexibilität, große Speicherplatzmengen je nach Bedarf zu verteilen und ohne Unterbrechung der Systemnutzung neue physikalische Laufwerke hinzuzufügen oder alte herauszunehmen. Der Acronis Backup & Recovery 11.5 Agent (S. 485) für Linux kann auf logische Volumes zugreifen, sie sichern und wiederherstellen, wenn er unter Linux mit 2.6-Kernel oder von einem Linux-basierten bootfähigen Medium (S. 487) ausgeführt wird.

Lokaler Backup-Plan

Backup-Plan (S. 486), erstellt auf einer verwalteten Maschine (S. 496) durch direkte Verwaltung (S. 489).

Lokaler Task

Ein auf einer verwalteten Maschine (S. 496) durch direkte Verwaltung (S. 489) erstellter Task (S. 495).

M

Management Server (Acronis Backup & Recovery 11.5 Management Server)

Zentraler Server zur Datensicherung innerhalb des Unternehmensnetzes. Acronis Backup & Recovery 11.5 Management Server versorgt den Administrator mit:

- einen zentralen Zugriffspunkt auf die Acronis Backup & Recovery 11.5-Infrastruktur
- einen einfachen Weg zur Sicherung von Daten auf zahlreichen Maschinen (S. 493) – durch Verwendung von zentralen Backup-Plänen (S. 498) und Gruppierung
- unternehmensweitem Monitoring und Berichtsfunktionalität
- der Fähigkeit, zentrale Depots (S. 498) zur Speicherung der Backup-Archive (S. 486) des Unternehmens zu erstellen
- der Fähigkeit, Storage Nodes (S. 495) zu verwalten
- einen zentralen Katalog (S. 488) aller Daten, die auf Storages Nodes gespeichert sind.

Gibt es mehrere Management Server im Netzwerk, dann arbeiten diese unabhängig voneinander, verwalten verschiedene Maschinen und verwenden verschiedene zentrale Depots zur Speicherung von Archiven.

Maschine

Ein physikalischer oder virtueller Computer, der eindeutig anhand seiner Betriebssysteminstallation identifiziert wird. Maschinen mit mehreren Betriebssystemen (Multi-Boot-Systeme) werden auch als mehrfache Maschinen betrachtet.

Media Builder

Spezielles Werkzeug zum Erstellen bootfähiger Medien (S. 487).

N

Nicht verwaltetes Depot

Jedes Depot (S. 489), das kein verwaltetes Depot (S. 496) ist.

P

Persönliches Depot

Lokales oder im Netzwerk befindliches Depot (S. 489), das durch direkte Verwaltung (S. 489) erstellt wurde. Sobald ein persönliches Depot erstellt wurde, erscheint auf der verwalteten Maschine eine Verknüpfung zu diesem in der Liste **Depots**. Mehrere Maschinen können den gleichen physikalischen Speicherort benutzen, z.B. ein freigegebenes Netzlaufwerk oder ein persönliches Depot.

Plan

Siehe Backup-Plan (S. 486).

R

Registrierte Maschine

Maschine (S. 493), die durch einen Management Server (S. 493) verwaltet wird. Eine Maschine kann zur gleichen Zeit nur auf einem Management Server registriert sein. Eine registrierte Maschine entsteht durch ein Verfahren zur Registrierung (S. 494).

Registrierung

Verfahren, das eine verwaltete Maschine (S. 496) zu einem Management Server (S. 493) hinzufügt.

Die Registrierung stellt eine Vertrauensstellung zwischen dem Agenten (S. 485) auf der Maschine und dem Server her. Während der Registrierung ruft die Konsole das Client-Zertifikat des Management Servers ab und leitet es an den Agent weiter, der es später beim Herstellen der Verbindung zur Authentifizierung benutzt. Dies hilft, Versuche von Angreifern des Netzwerks zu verhindern, eine Verbindung unter Vortäuschung eines vertrauten Auftraggebers (des Management Servers) herzustellen.

Replikation

Eine Replikation entspricht dem Kopieren eines Backups (S. 485) zu einem anderen Speicherort. Das Backup wird standardmäßig direkt nach seiner Erstellung kopiert. Durch die Konfiguration einer Inaktivitätszeit erhält der Benutzer die Option, das Kopieren des Backups aufzuschieben.

Diese Funktion ersetzt und erweitert die Backup-Option 'Dual-Destination', wie sie in Acronis Backup & Recovery 10 verfügbar war.

S

Single-Pass-Backup

Ein Single-Pass-Backup (Einzeldurchlauf-Backup, auch als anwendungssensitives Backup bekannt) ist ein Laufwerk-Backup, welches Metadaten von VSS-kompatiblen Anwendungen enthält, die auf dem Laufwerk vorliegen. Diese Metadaten ermöglichen es, die per Backup gesicherten Anwendungsdaten zu durchsuchen und wiederherzustellen, ohne das komplette Laufwerk oder Volume wiederherstellen zu müssen.

Standardgruppe

Eine Gruppe von Maschinen, die permanent auf einem Management Server (S. 493) vorliegen.

Diese eingebauten Standardgruppen können nicht gelöscht, zu anderen Gruppen verschoben oder manuell modifiziert werden. Benutzerdefinierte Gruppen können nicht innerhalb von Standardgruppen erstellt werden. Es gibt keinen anderen Weg, eine Maschine aus der Standardgruppe zu entfernen, als diese vom Management Server zu entfernen.

Statische Gruppe

Maschinengruppe, die der Administrator eines Management Servers (S. 493) durch manuelles Hinzufügen von Maschinen zur betreffenden Gruppe auffüllt. Eine Maschine verbleibt in einer statischen Gruppe, bis der Administrator diese von der Gruppe oder vom Management Server entfernt.

Storage Node (Acronis Backup & Recovery 11.5 Storage Node)

Server, der zur optimierten Nutzung verschiedener Ressourcen gedacht ist, die zum Schutz von Unternehmensdaten erforderlich sind. Dieses Ziel wird durch die Organisation von verwalteten Depots (S. 496) erreicht. Dank eines Storage Nodes kann ein Administrator:

- einen einzelnen zentralen Katalog (S. 488) für alle in verwalteten Depots gespeicherte Daten verwenden
- verwaltete Maschinen (S. 496) von unnötiger CPU-Last befreien, indem Bereinigungen (S. 487), Validierungen (S. 496) und anderen Aktionen mit den Backup-Archiven (S. 486) durchgeführt werden, die sonst von den Agenten (S. 485) ausgeführt würden
- den von Archiven (S. 486) verursachten Backup-Datentransfer und belegten Speicherplatz durch Verwendung von Deduplizierung (S. 488) drastisch senken
- mit Hilfe verschlüsselter Depots (S. 496) den Zugriff auf Backup-Archive verhindern, auch wenn das Speichermedium gestohlen wird oder es zu unbefugtem Zugriff auf die Archive kommt.

T

Task

Ein Satz von Aktionen, der von Acronis Backup & Recovery 11.5 zu einem bestimmten Zeitpunkt oder auf ein Ereignis hin durchgeführt wird. Die Aktionen sind in einer nicht vom Benutzer lesbaren Service-Datei beschrieben. Zeitpunkt oder Ereignis (für die Planung) werden in einem geschützten Registry-Schlüssel (in Windows) oder im Dateisystem (in Linux) gespeichert.

Türme von Hanoi

Populäres Backup-Schema (S. 487), das für ein ideales Gleichgewicht zwischen der Größe eines Backup-Archivs (S. 486) und der Anzahl von Wiederherstellungspunkten (S. 497) sorgen soll, die im Archiv enthalten sind. Im Gegensatz zum GVS (S. 491)-Schema, das lediglich drei Level für die Wiederherstellungsauflösung hat (täglich, wöchentlich und monatlich), ist es mit dem Schema „Türme von Hanoi“ möglich, den zeitlichen Abstand zwischen Wiederherstellungspunkten bei steigendem Alter des Backups kontinuierlich zu reduzieren. Das ermöglicht eine sehr effiziente Verwendung des Backup-Speichers.

Weitere Informationen finden Sie unter Backup-Schema „Türme von Hanoi“ (S. 76).



Validierung

Aktion, mit der die Möglichkeit einer Datenwiederherstellung aus einem Backup (S. 485) geprüft wird.

Die Validierung eines Datei-Backups imitiert die Wiederherstellung aller Dateien aus einem Backup an einen imitierten Zielort. Die Validierung eines Laufwerk-Backups berechnet eine Prüfsumme für jeden Datenblock, der im Backup gespeichert ist. Beide Prozeduren sind ressourcenintensiv.

Obwohl eine erfolgreiche Validierung eine hohe Wahrscheinlichkeit für eine erfolgreiche Wiederherstellung bedeutet, werden nicht alle Faktoren geprüft, die eine Wiederherstellung beeinflussen. Wenn Sie das Betriebssystem gesichert haben, kann nur eine testweise Wiederherstellung unter Verwendung eines bootfähigen Mediums auf einem Ersatzlaufwerk eine zukünftige erfolgreiche Wiederherstellung garantieren.

Verschlüsseltes Archiv

Ein Backup-Archiv (S. 486), das nach dem Advanced Encryption Standard (AES) verschlüsselt ist. Ist die Verschlüsselungsoption und ein Kennwort für das Archiv in den Backup-Optionen (S. 486) definiert, dann wird jedes zum Archiv gehörende Backup vom Agenten (S. 485) noch vor dem Ablegen des Backups am Zielort verschlüsselt.

Verschlüsseltes Depot

Verwaltetes Depot (S. 496), bei dem ein Storage Node (S. 495) alles dorthin Geschriebene verschlüsselt bzw. alles von dort Gelesene transparent entschlüsselt, wobei ein für das Depot spezifischer Encryption Key benutzt wird, der auf dem Knoten gespeichert ist. Falls das Speichermedium gestohlen wird oder eine unbefugte Person darauf zugreift, wird der Übeltäter den Inhalt des Depots ohne Zugriff auf den Storage Node nicht entschlüsseln können. Verschlüsselte Archive (S. 496) werden über die Verschlüsselung des Agenten (S. 485) erstellt.

Verwaltete Maschine

Physikalische oder virtuelle Maschine (S. 493), auf der wenigstens ein Acronis Backup & Recovery 11.5 (S. 485) Agent installiert ist.

Verwaltetes Depot

Ein zentrales Depot (S. 498), welches von einem Storage Node (S. 495) verwaltet wird. Auf Archive (S. 486) in einem verwalteten Depot kann folgendermaßen zugegriffen werden:

bsp://knoten_adresse/depot_name/archiv_name/

Physikalisch können sich verwaltete Depots auf einem freigegebenen Netzlaufwerk, einem SAN, NAS, auf einer lokalen Festplatte des Storage Nodes oder einer Bandbibliothek befinden, die lokal an den Storage Node angeschlossen ist. Der Storage Node führt Bereinigungen (S. 487) und Validierungen (S. 496) für jedes im verwalteten Depot gespeicherte Archiv durch. Ein Administrator kann zusätzliche Aktionen spezifizieren, die der Storage Node durchführen soll, z.B. Deduplizierung (S. 488) oder Verschlüsselung.

Virtuelle Maschine

Auf dem Acronis Backup & Recovery 11.5 Management Server (S. 493) wird eine Maschine (S. 493) als 'virtuell' betrachtet, wenn sie per Backup vom Virtualisierungshost gesichert werden kann, ohne dass dafür der Agent (S. 485) auf der Maschine installiert sein muss. Solche Maschinen erscheinen im Abschnitt **Virtuelle Maschinen**. Falls ein Agent im Gastsystem installiert ist, erscheint die Maschine im Abschnitt **Maschinen mit Agenten**.

Voll-Backup

Selbstständiges Backup (S. 485), das alle Daten enthält, die für die Sicherung gewählt wurden. Sie benötigen kein weiteres Backup, um die Daten aus einem Voll-Backup wiederherzustellen.

W

Wiederauffüllbarer Pool

Ein Band-Pool, der bei Bedarf Bänder aus dem Pool **Frei Bändern** entnehmen darf.

Wiederherstellungspunkt

Tag und Zeitpunkt, zu dem die gesicherten Daten wiederhergestellt werden können.

WinPE (Windows Preinstallation Environment)

Ein minimales, funktionsreduziertes Windows-System, welches üblicherweise von OEMs und Unternehmen für Deployments, Tests, Diagnosen und Systemreparaturen verwendet wird. Eine Maschine kann in die WinPE über PXE, CD-ROM, USB-Flash-Laufwerke oder Festplatten gebootet werden. Das Acronis Plug-in für WinPE (S. 484) ermöglicht die Ausführung des Acronis Backup & Recovery 11.5 Agenten (S. 485) in der Preinstallation Environment.

Z

Zentrale Verwaltung

Verwaltung der Acronis Backup & Recovery 11.5-Infrastruktur durch eine zentrale Verwaltungseinheit, die Acronis Backup & Recovery 11.5 Management Server (S. 493) genannt wird. Die zentralen Verwaltungsaktionen umfassen:

- Erstellung zentraler Backup-Pläne (S. 498) für registrierte Maschinen (S. 494) und Maschinengruppen
- Erstellung und Verwaltung statischer (S. 495) und dynamischer Gruppen (S. 490) von Maschinen (S. 493)
- Verwaltung von auf den Maschinen existierenden Tasks (S. 495)

- Erstellung und Verwaltung zentraler Depots (S. 498) zur Speicherung von Archiven
- Verwaltung von Storage Node (S. 495)
- Überwachung der Aktivitäten der Acronis Backup & Recovery 11.5 Komponenten, Erstellung von Berichten, Einsicht in das zentrale Log und mehr.

Zentraler Backup-Plan

Ein Backup-Plan (S. 486), der vom Management Server (S. 493) auf eine verwaltete Maschine (S. 496) verteilt wird. Ein solcher Plan kann nur durch Bearbeitung des ursprünglichen Backup-Plans auf dem Management Server modifiziert werden.

Zentraler Task

Ein Task (S. 495), der vom Management Server (S. 493) auf eine Maschine verbreitet wird. Ein solcher Task kann nur durch Bearbeitung des ursprünglichen Tasks oder zentralen Backup-Plans (S. 498) auf dem Management Server modifiziert werden.

Zentrales Depot

Ein Speicherort im Netzwerk, der vom Administrator des Management Servers (S. 493) zugeteilt wird, um als Speicherplatz für Backup-Archive (S. 486) zu dienen. Ein zentrales Depot kann von einem Storage Node (S. 495) verwaltet werden oder es ist nicht verwaltet. Die Gesamtzahl und Größe der Archive, die in einem zentralen Depot gespeichert werden können, wird nur von der Speicherplatzgröße begrenzt.

Sobald der Administrator ein zentrales Depot erstellt, werden dessen Name und der Pfad zum Depot an alle auf dem Server registrierten Maschinen (S. 494) verteilt. Die Verknüpfung zum Depot erscheint auf den Maschinen in der Liste **Depots**. Jeder Backup-Plan (S. 486), der auf den Maschinen existiert, einschließlich der lokalen Pläne, kann das zentrale Depot benutzen.

Auf einer Maschine, die nicht auf dem Management Server registriert ist, kann ein Benutzer mit entsprechenden Rechten Backups zum zentralen Depot ausführen, wenn er den vollen Pfad zum Depot verwendet. Wenn das Depot verwaltet wird, werden die Archive des Benutzers vom Storage Node ebenso wie andere Archive behandelt, die im Depot gespeichert worden sind.